A FRAMEWORK FOR SECURE HUMAN COMPUTER INTERACTION

by

JAMES JOHNSTON

DISSERTATION

submitted in the fulfilment of the requirements for the Degree

MAGISTER SCIENTIAE

in

COMPUTER SCIENCE

at the

RAND AFRIKAANS UNIVERSITY

SUPERVISOR
PROF L LABUSCHAGNE
OCTOBER 2004

Summary

This research is concerned with the development of a framework for the analysis and design of interfaces found in a security environment. An example of such an interface is a firewall. The purpose of this research is to use the framework as a method to improve the usability of an interface, thus aiding the user to implement the correct security features. The purpose is also to use the framework to assist in the development of trust between a user and a computer system. In this research the framework comprises six criteria which are used to analyse interfaces found in the traditional software environment, Internet banking environment and e-commerce environment.

In order to develop the framework an overview of the fields of information security and human computer interfaces (HCI) is given. The overview provides background information and also establishes the existing research which has been done in these fields.

Due to its popularity, the Windows Internet Connection Firewall is analysed in this research. Based on the criteria a level of trust fostered between the user and interface is calculated for the firewall. It is then shown how this level of trust can be improved by modifying the interface. A proposed interface for the firewall is presented according to the criteria.

Interfaces found in the online Internet environment are discussed. This is important in order to identify the similarities and differences between traditional software interfaces and web interfaces. Due to these differences the criteria are modified to be relevant in the analysis and design of security interfaces found on the Internet.

Three South African online banking websites are analysed according to the modified framework. Each interface is broken down into a number of components which are then analysed individually. The results of the analysis are compared between the three banking sites to identify the elements which make up a successful interface in an online banking environment.

Lastly, three interfaces of e-commerce websites are analysed. Recommendations are made on how the interfaces can be improved, thus leading to a higher level of trust.

Acknowledgments

I would like to thank my supervisor Professor Labuschagne for his guidance, insight, encouragement and time.

I am grateful to my parents for their love and generosity to me throughout my university career.

Table of Contents

Index of Figures

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Chapter 9

Index of Tables

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Chapter 9

Chapter 1
Introduction

Computers continue to play a vital role in society. Over the past 50 years the use of computers has grown to the point where they are present in almost every aspect of daily life. The first computers, such as the ENIAC, had a very limited user interface, with instructions being given to the computer via a card reader [WEIK61]. Due to the small number of computers, only a few scientists and academic staff had access to them. The complicated interfaces also meant that only a handful of people knew how to operate computers like the ENIAC. The operation of computers became easier with the introduction of a mouse and keyboard on the first commercial computer in 1960 [POLS04]. This led to computers being more widely used. However, they were still prohibitively expensive (about $120 000) and instructions were given to the computer via text-based commands. The 1980s saw an explosion in the number of personal computers due to the combination of lower prices and the introduction of graphical user interfaces. This trend has continued into the new millennium with computers and technology becoming cheaper and easier to operate. This in turn leads to technology being accessible to more people.

In today's world users continue to experience technology through various user interfaces – mobile phone menus; buttons, icons and windows on a computer screen; dials and knobs in cars; back buttons and hyper links on the Internet. These interfaces are normally designed to aid the user's experience. For example, a well designed interface assists the user in becoming proficient in the operation of a software program in a shorter time frame. This causes the user to become more efficient in completing a task. The user feels in control and satisfied with the technology. On the other hand, a poorly designed interface can frustrate the user and hinder the completion of tasks. This may build feelings of distrust and scepticism in the user towards the system.

Initially during the 1960s and 1970s information security was not a huge concern due to the small number of computers and the limited number of users who were able to operate the available computers. However, with the increase in the number of computers during the 1980s and 1990s illegal and malicious activity has become more proliferate. The new millennium has seen the importance of computer and information security continue to grow as the world becomes more connected and increasing amounts of business are transacted electronically. According to the Computer Crime and Security Survey [RICH03], the most popular security technologies used by companies are anti-virus software (99% of companies polled use it) and firewalls (used by 98% of companies polled). The importance of these security technologies is highlighted in that 56% of the respondents indicated some form of unauthorised use of their computer systems. A further 15% of the companies surveyed stated that they did not know whether there had been any unauthorised use of their computer systems over the past year. The leading form of attack or misuse was viruses (82% of companies affected) followed by insider abuse of Internet access (80% of companies affected). A total of $201 million was lost by the 251 companies which suffered security breaches. Even though most of the companies are using firewalls, 36% reported at least one system penetration. This is partly due to faulty technology but also due to the incorrect installation and use of the software. This means that the role of interfaces which convey and guide the user through security features is crucial. The field of human computer interaction (HCI) has traditionally been concerned with the development of user-friendly interfaces. Security needs to grow along with the growth in the number of interfaces.

In this chapter the problem statement is first given. This is followed by the research goal and research objectives. The project deliverables are then presented along with a discussion of the research methodology used in this dissertation. The chapter structure of the dissertation is then outlined.

1.1 Problem statement

The user experiences security functionality through the interface. The interface informs the user of the security functions that are available and how to use them. For example, an email program which allows the encryption of messages needs to give a description of encryption, be easy to use and inform the user whether the sent email has been encrypted. Often security is not a priority for users, which means that if it is too difficult to use, a security feature will not be used.

Often when it comes to security, the 'weakest link' is the user. A user may write down their passwords and stick them on their computer monitor or even store them in a text file on their hard drive. This means that even if the technical security features of a system are robust, the overall security is weak because of the user. Some users may not be aware of a security feature or may use it incorrectly. For example, a personal firewall can only protect a user's computer if it is active, and it will only be active if the user knows how to turn it on. The interface needs to ensure that the user is guided to minimise the potential for the user to be the 'weakest' link. Many users do not receive any formal training in the use of security software. Adding these factors together creates a problem where the interface could impact the security of a system.

The problem is that there is currently no method to evaluate an interface from an information security perspective. Interface design criteria are also not available to assist in the design of new interfaces and the improvement of existing interfaces in an information security environment.

1.2 Research goal

The goal of this research is to develop a formal framework which can be used to evaluate and improve the interface of an application and thereby improve the security of a system.

This research focuses on the aspects of HCI that are relevant in a security environment. An example of this is the interface of a software product such as an encryption program or a firewall. These applications deal almost exclusively with security functions. Other interfaces also have parts of them which deal with security, such as the interface of a banking or e-commerce website.

1.3 Research objectives

In order to achieve the research goal stated above, a number of objectives will need to be met. The first objective is to determine the current status of HCI within security applications and to establish if there are adequate criteria that can be used to develop secure HCI. This objective will be achieved by completing a literature review of the fields of HCI and security. It is important to identify the existing research and to establish if it is sufficient or how it can be adapted and extended to apply to the field of HCI in a security environment. Particular attention will be given to the identification of acceptable criteria in the HCI field which are used to develop and analyse general user interfaces.

The second objective is to develop formal criteria, called HCI-S criteria, which specifically focus on interfaces in an information security environment. Principles from HCI and information security will be combined to form the HCI-S criteria. A definition of HCI-S for the purposes of this research will be developed.

The third objective is to apply the proposed HCI-S criteria to an actual security interface. To achieve this objective the interface of a firewall will be analysed using the HCI-S criteria. The aim of this analysis is to attempt to quantify the level of trust which the interface fosters. The criteria will also be used to generate recommendations on how the interface of the firewall can be modified to improve trust.

The fourth objective is to establish the applicability of HCI and HCI-S to an Internet banking interface. An Internet banking interface differs from a standard security interface in that the banking interface must generate a much higher level of trust due to the nature of banking.

The fifth objective is to test the applicability of HCI-S criteria to an e-commerce environment. In order to achieve this objective the HCI-S criteria will be used to analyse e-commerce interfaces, quantifying the level of trust and providing recommendations for improvement.

The achievement of an objective will produce a deliverable as discussed in the next section.

1.4 Deliverables

Each research deliverable correlates to one research objective. The deliverables from the objectives above are the following:

Objective 1: The first deliverable is a generally accepted definition of HCI and a literature summary of what constitutes current HCI criteria.

Objective 2: The second deliverable is a set of specific HCI-S criteria which are focused on interfaces in a security environment.

Objective 3: The third deliverable is proof that the HCI-S criteria can be applied successfully in a traditional application environment. This proof will be evident by the analysis of the Internet Connection Firewall and then by the calculation of a level of trust for the firewall.

Objective 4: The fourth deliverable is the HCI-S criteria modified so that they are relevant to the Internet banking environment and a level of trust calculated for three interfaces found in the online banking environment.

Objective 5: The fifth deliverable is proof that the HCI-S criteria can also be applied successfully in an e-commerce environment. As with the third deliverable, a level of trust for each web interface analysed will be calculated.

In the next section the research approach is discussed.

1.5 Approach

The beginning phase of this research is made up of a thorough literature investigation into the fields of HCI and security. The purpose of this investigation is to establish the common ground between these two fields.

During the analysis of various user interfaces qualitative research is mainly used. This is because the human operation of interfaces must be studied in context. Currently the number of theories available to explain the behaviour of users in the field of HCI-S is limited and this topic therefore lends itself to qualitative research. During the qualitative research inductive reasoning is used. A specific interface is analysed and observations made as to what forms a successful interface. Based on the observations, inferences are made about other similar interfaces [STRAU04]. Recommendations for the interfaces are generally made in words. However, some figures are also used to substantiate the findings [MILE04].

The case study form of qualitative research has been chosen [HENN04]. This is because the analysis of interfaces lends itself to the study of specific interfaces. Each case study is limited with the focus being on an individual interface and then similar interfaces found in the environment. Different case studies have been chosen in order to show different perspectives of the problem. An embedded analysis is used, focusing only on the interfaces of software. At the end the "lessons learned" are presented as to what constitutes a successful interface in a particular environment [HENN04].

The weakness with qualitative research is that it can be subjective and is open to the influences of the researcher's own opinions. The next step in this research, which is beyond the scope of this dissertation, would be to include field testing of interfaces to see if there is a correlation between the level of trust according to the HCI-S criteria and the user's ability to accomplish tasks.

Both action and predictive research are used in this research. The practical application of how the problem can be solved is demonstrated through the implementation of the HCI-S criteria. The predicted outcome of using the HCI-S criteria is that the interface will improve [STRAU04]. Quantitative research techniques are used to validate the prediction.

Quantitative research is used in a limited capacity to calculate the level of trust generated by security interfaces. Various controls based on the HCI-S criteria are developed and used to calculate a percentage which represents trust. Deductive reasoning is used during quantitative research in which a conclusion is reached by using logical arguments [HENN04].

In the next section the structure of the research is presented.

1.6 Structure of the dissertation

This research is composed of ten chapters. Chapter 1 is the introduction, which includes the problem statement and research objectives. This is followed by chapter 2, which provides background information to the field of HCI. In chapter 3 the field of information security is discussed. The new field of HCI-S is introduced in chapter 4, along with the HCI-S criteria. The HCI-S criteria are then used in chapter 5 to analyse the Windows XP Internet Connection Firewall. Chapter 6 follows with recommendations on how the Internet Connection Firewall can be improved. Chapter 7 provides a platform for the analysis of interfaces found on the Internet. In chapter 8 the interfaces of three banking websites are analysed and recommendations given. This is followed in chapter 9 by the analysis of three e-commerce websites, along with recommendations. Chapter 10 is the conclusion.

Figure 1.1 shows the possible order in which this dissertation can be read. The chapters have been colour-coded. Chapters of the same colour form a unit and should be examined together.

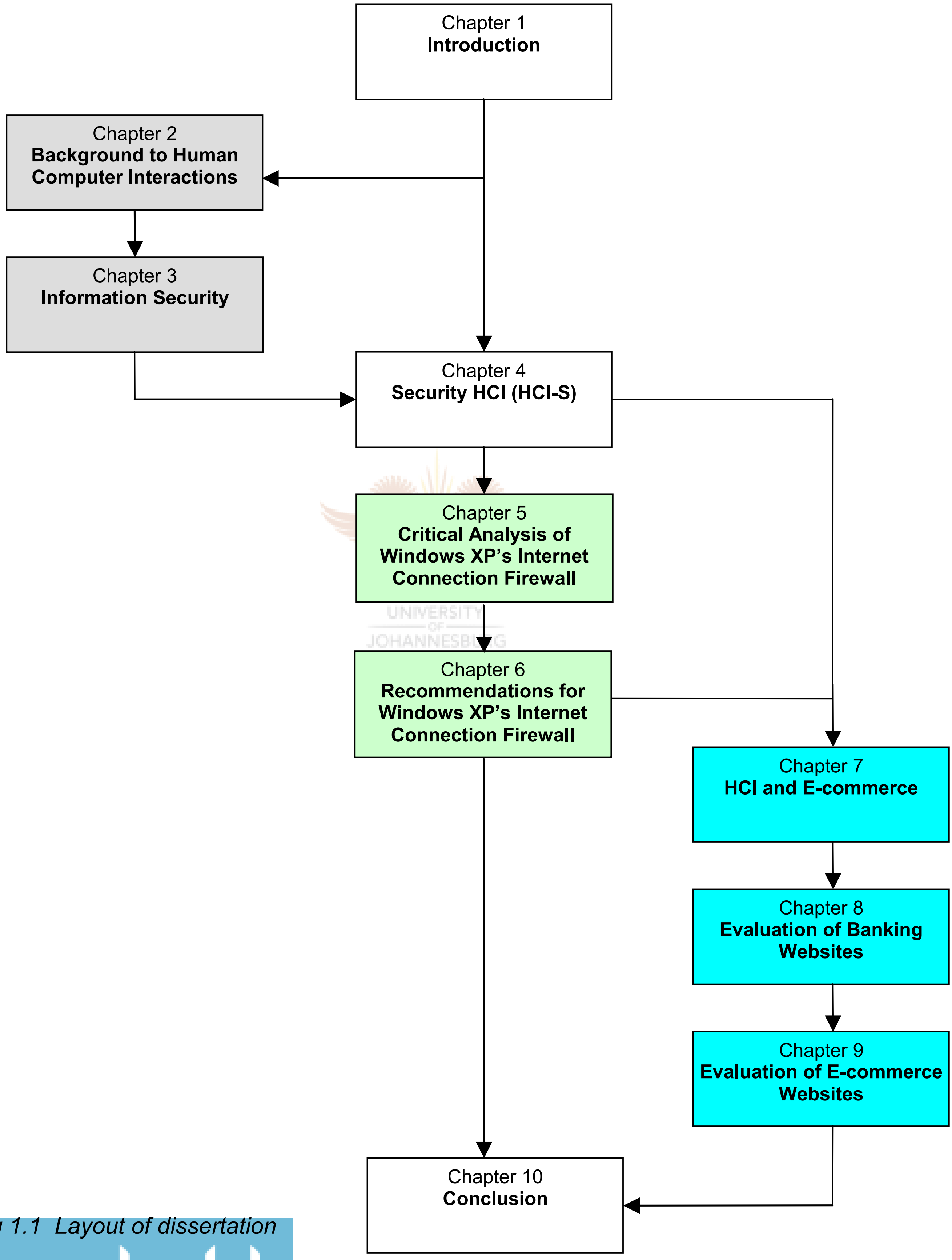

Chapter 1
Introduction
Chapter 2
Background to Human Computer Interactions
Chapter 3
Information Security
Chapter 4
Security HCI (HCI-S)
Chapter 5
Critical Analysis of Windows XP's Internet Connection Firewall
Chapter 6
Recommendations for Windows XP's Internet Connection Firewall
Chapter 7
HCI and E-commerce
Chapter 8
Evaluation of Banking Websites
Chapter 9
Evaluation of E-commerce Websites
Chapter 10
Conclusion

Fig 1.1 Layout of dissertation

As can be seen from figure 1.1, chapter 4 is a crucial chapter and the main focus of this dissertation. Chapters 2 and 3 provide the platform for chapter 4. Chapters 5, 6, 8 and 9 implement the principles developed in chapter 4.

A brief summary of each chapter follows.

Chapter 1: The aim of this chapter is to outline the problem statement and research objectives to provide a backdrop to the dissertation.

Chapter 2: The aim of this chapter is to provide an overview of HCI. In order to achieve this aim, a number of objectives will need to be met. The first objective of chapter 2 is to find a generally accepted definition of HCI and usability. Once this is achieved the second objective is to identify the current standards for HCI and usability. The third objective is to establish the criteria of a successful HCI which have already been developed in the field of usability. These criteria are then modified in future chapters.

Chapter 3: The aim of this chapter is to provide an overview of information security. A number of objectives will need to be met in order to achieve this aim. The first objective is to find a generally accepted definition of information security. The second objective is to then identify the current security standards and to establish the research that has already been done in the field of information security. The third objective is to identify a framework for security which relates to HCI.

Chapter 4: The aim of this chapter is to develop HCI-S criteria so that they can be used in future chapters to analyse existing interfaces. The first objective of this chapter is to introduce a new term 'HCI-S'. HCI-S was not found in any other literature and a definition is therefore established. The second objective of this chapter is to define the HCI-S criteria so they can be used by developers to design better security interfaces.

Chapter 5: The goal of this chapter is to use the HCI-S criteria to critically analyse an interface found in an information security environment. Microsoft Windows XP's Internet Connection Firewall (ICF) is analysed. The purpose of this is to see how the HCI-S criteria can be applied in a real-world context. The first objective of this chapter is to examine the ICF interface during activation, configuration and operation so that the interface can be analysed according to HCI-S criteria. Following from the examination of the ICF, the second objective is then to draw conclusions based on the HCI-S criteria to form a base from which recommendations can be made in the following chapter. The third objective is to identify the advantages and disadvantages of using the HCI-S criteria in order to determine their completeness.

Chapter 6: In this chapter recommendations are given on how the ICF's interface can be improved. The aim of this chapter is to show how the ICF's interface can be changed to improve the security of a system by making it easier to use. In order to achieve the goal, three objectives are set. The first objective is to improve the interface during the activation of the ICF, which should lead to better security. The second objective is to modify the interface so that the configuration of the ICF is easier. The third objective is to change the interface during the operation of the ICF so that it is more intuitive to use and that the user is made aware of the presence of the ICF.

Chapter 7: Chapter 7 focuses on security interfaces found in an online environment. The aim of this chapter is to develop the HCI-S criteria further so that they may be used to analyse security interfaces found in an e-commerce environment. In order to achieve this goal, a number of objectives need to be met. The first objective of this chapter is to see whether HCI principles play an important role in a web-based environment. Once this has been achieved, the second objective is to determine if the HCI-S criteria need to be adapted so that they can be used in a web environment. This is necessary because the HCI-S criteria are used in later chapters to analyse interfaces found on the Internet. The third objective is to determine which functional components of a website relate to information security and which HCI-S criteria apply to each functional component.

Chapter 8: The aim of this chapter is to use the HCI-S criteria to calculate the level of trust which various online banking websites foster. In order to achieve this aim, three objectives need to be met. The first objective is to use the HCI-S criteria to analyse the components found on three banking websites. Once the interfaces have been analysed, the second objective is to attempt to quantify the level of trust which each interface fosters. The third objective is to attempt to identify the reasons why certain banking interfaces foster a higher level of trust than others.

Chapter 9: The aim and objectives of this chapter are similar to those of chapter 8. Chapter 8 focused on the security interface of banking sites, and chapter 9 focuses on the security interfaces of e-tailers and online services sites. The aim of the chapter is to use the HCI-S criteria to calculate the level of trust fostered by each online interface. In order to accomplish this aim, each interface first needs to be analysed according to the HCI-S criteria. The second objective is then to attempt to quantify the level of trust fostered by each interface based on the analysis. The last objective is to try to pinpoint the reasons why some interfaces foster a higher level of trust than others.

Chapter 10: Chapter 10 is the conclusion to this dissertation. In the conclusion the strengths and weaknesses of the HCI-S criteria are discussed. The value of this research is also presented along with the direction of possible further research.

This research sets out to find a way to improve the security of a system by examining the human computer interface of the system.

In the next chapter the field of HCI is explored.

Chapter 2
Background to Human Computer Interaction

2.1 Introduction

HCI stands for human computer interaction. From the computer science perspective HCI deals with the interaction between one or more humans and one or more computers. An image which comes to mind is that of a person using a graphical interface (e.g. Microsoft Windows) on a workstation. It is clear, however, that HCI encompasses more than this, depending on the definition of the terms 'human', 'computer' and 'interaction' [HEWE96].

The aim of this chapter is to provide an overview of HCI. In order to achieve this aim, three objectives are set. The first objective of this chapter is to find a generally accepted definition of HCI and usability. Once this is achieved, the second objective is to identify the current standards for HCI and usability. The third objective is to establish the criteria of a successful HCI.

This chapter begins with a brief history of HCI. A definition of HCI is given, followed by a definition of usability. Standards in HCI are discussed next. In conclusion criteria for a successful HCI are given. These criteria are adapted in future chapters to suit the focus of this dissertation.

2.2 Brief history of HCI

With the start of the industrial age and the development of machinery and factories, research into how humans and machines interact started. The Second World War provided the catalyst for the intensification of research into human machine interaction to assist in the development of more effective weapons. During this period machines were being developed with more and more electronic components. In 1949 the Ergonomics Research Society was formed. This society at the time was mainly focused on the physical characteristics of machines and systems and how these affect the user's performance [ALAN98].

The direct manipulation of visible objects on the screen with a pointing device was first demonstrated by Ivan Sutherland in 1963. This demonstration formed part of his MIT PhD thesis - SketchPad [SUTH63]. Using a light-pen Sutherland was able to grab, move and change the size of objects. The introduction of graphical user interfaces helped to develop the field of HCI.

The first conference on HCI was held in Gaithersburg in 1982. This conference focused on human factors in computing and led to the first Association for Computing Machinery Special Interest Group on Computer-Human Interaction (ACM SIGCHI) [SIGCHI02]. This conference coincided with the emergence of the personal computer. Over the past 22 years research into computer interfaces and the use of computers has grown.

In 1988 Norman developed a simplistic but influential model in the HCI field. His model outlined the stages of interaction between a human user and a computer. The basics of the model are [NORM88]:

1. User formulates a plan of action
2. User executes plan of action using the computer interface
3. After the plan has been executed the user observes the computer interface to evaluate the results of the plan
4. Further actions are determined.

Jakob Nielsen, a usability expert, developed a set of ten guidelines for designing interfaces in 1993. These criteria are discussed later in section 2.6 as they form a key base for this research into HCI in a security environment [BRINCK02].

The 1990s saw the explosion of the World Wide Web. In 1993 there were only 130 websites [ZAKON04]. By June 2004 this figure had grown to over 250 million websites with over 700 million users [GROW04]. With the huge growth in the number of users, the usability and user-friendliness of web interfaces have become critically important. Web browsers are becoming the standard for interbusiness and personal communication [BRINCK02].

In the next section a definition of HCI for this dissertation is formulated.

2.3 Definition of HCI

In this dissertation the following definitions of human, computer and interaction are used [ELOF02]:

Human - the user is any person who uses technology in order to accomplish a specific task.

Computer - the physical hardware that runs the specific software.

Interaction - the way the human communicates with, uses and reacts to the technology.

HCI is an interdisciplinary subject. It has aspects of computer science (application design and engineering of human interfaces), psychology (cognitive processes and the analysis of user behaviour), sociology and anthropology (link between technology, people, work and organisations) and industrial design (the physical design of computer peripherals) (figure 2.1). For this text HCI is approached primarily from a computer science and information security point of view. However, HCI is framed broadly enough so as not to ignore the context of the subject. The other disciplines are viewed as supporting disciplines.

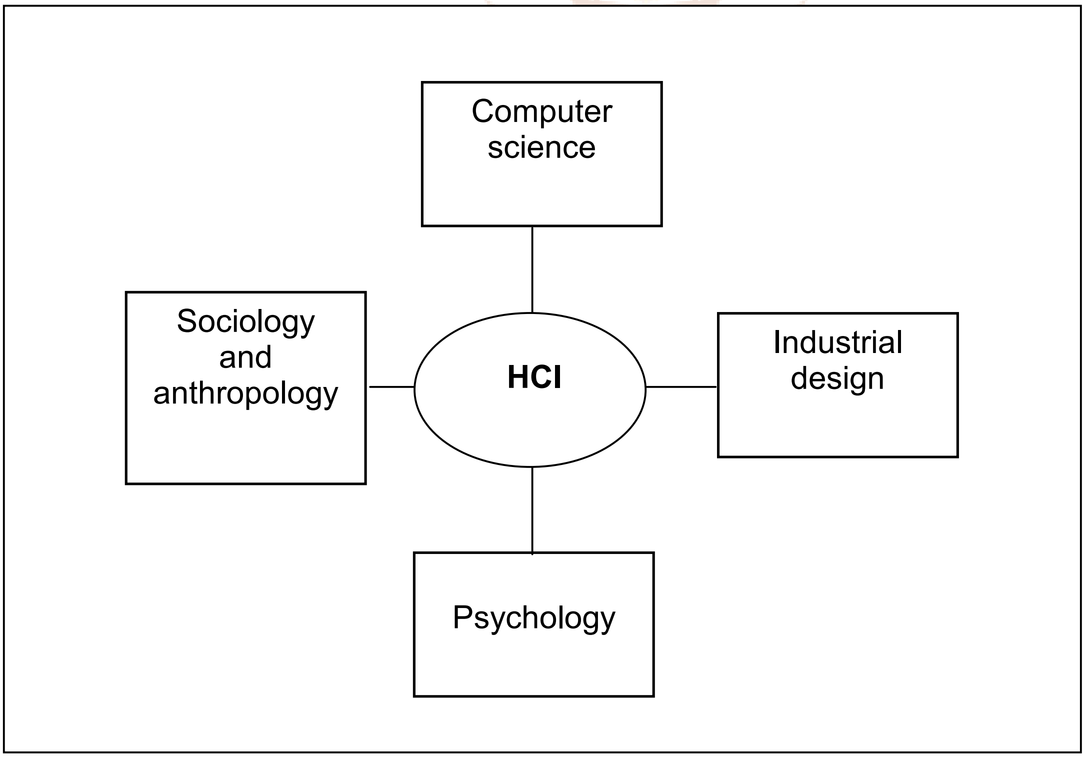


Fig 2.1 HCI is an interdisciplinary subject

The field of HCI is very broad and can encompass all forms of interaction between humans and machines. An important part of HCI is usability, which is defined in the next section (2.4). Below are some definitions of HCI, followed by a definition of HCI which is

used for this dissertation.
According to Michels [MICH95], HCI can be defined as:

"The part of a computer program responsible for establishing the common ground with a particular (i.e. well-known) user. His task is accomplished by expanding and maintaining this common ground throughout the interaction process with the application. Whenever possible, direct manipulation of familiar objects should be the leading interaction principle."

This definition mentions the 'direct manipulation of familiar objects'. This is possible if these objects are known from the real world or from other HCIs. It also hints at the goal of an HCI, which is to facilitate the interaction between the user and computer.

Another definition of HCI [adapted from ALAN98] is:

HCI is the process of communication (direct and indirect) between a user and a computer dealing with the physical and psychological aspects of this process.

This definition highlights two important aspects of HCI:

The physical aspect
This deals with the physical capabilities and limitations of the user. For example, about 8% of males and 1% of females suffer from colour blindness, with most being unable to discriminate between red and green [ALAN98]. Users are also more sensitive to movement in their peripheral visions. This means that if a user is focusing on a particular position on a computer screen, a flashing image on the side will attract their attention [SUTCLI95].

A user receives inputs through sight, sound and touch. These inputs then need to be interpreted and processed, which forms part of the psychological aspect of HCI.

The psychological aspect
This is the cognitive process of how users interpret information. Information which is received via the senses is stored temporarily in the user's sensory or working memory, or permanently in long-term memory [ALAN98]. This information can then be processed leading to reasoning, problem-solving, thinking and learning [SUTCLI95]. Presenting information in a logical order can help to make the processing of information easier for a

user. Grouping information together can also make it easier for a user to recall. Most users can recall from short-term memory seven chunks or groups of information [MILL56]. For example, 082 847 9834 is easier to recall than 0728492837.

Factors such as attention, stress and fatigue can aid or hamper the cognitive process.

Definition of HCI for this dissertation

For this dissertation a more narrow definition of HCI is used:

HCI deals with the interface which a human uses to interact with a computer.

The 'interface' is a web interface or a traditional graphical user interface on a computer. The 'computer' in this definition is an electronic device which a user interacts directly with, for example a traditional home computer, office personal computer, a personal digital assistant (PDA) or a cell phone.

The term 'usability' is discussed in the next section.

2.4 Definition of usability

As mentioned in the previous section, an important part of HCI is usability. The usability of a system is how well it supports people in doing their tasks and activities [GOV1].

A more formal definition, according to ISO 9241 (Ergonomic Requirements for Office Work with Visual Display Terminals) [ISO9241], is:

"Usability is the extent to which a product can be used to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use."

According to Tom Brinck [BRINCK02], usability is the product of six design goals:

1. Functionally correct: A system is only usable if it performs the functions that a user needs.
2. Efficient to use: The time taken to perform actions should be kept to a minimum.
3. Easy to learn: The operation of a system should be intuitive and contain as few

steps as possible.

4. Easy to remember: The system should not tax the user's memory.
5. Error tolerant: A system should firstly attempt to pre-empt errors. Secondly, if errors do occur, they should be easy to detect and identify. Thirdly, errors should be easy to correct by the user once they have been identified.
6. Subjectively pleasing: This goal takes into account how a user feels using a system. This goal is often very personal.

Depending on the nature of the system, a different goal may take precedence. For example, a nuclear power plant system would have error tolerance as its primary usability goal, while a computer game would have subjectively pleasing as its main goal [BRINCK02].

As can be seen from the above goals, the terms ‘HCI’ and ‘usability’ are similar. For the purposes of this dissertation, the two terms are used interchangeably.

In the next section standards in the field of HCI are discussed.

2.5 Standards for HCI and usability

In this section the importance of HCI standards, the contents of HCI standards, the different types of HCI standards and the difficulties in applying HCI standards are discussed.

2.5.1 Importance of HCI standards

HCI standards provide a uniform look and feel for user interfaces. This means that all products for a particular platform should be similar. For example, Microsoft Windows follows certain interface design guidelines in that elements such as buttons and windows behave in the same manner [BUIE99].

Standardisation facilitates learning and reduces errors by taking advantage of knowledge the users have gained from other products and similar situations. If a user knows how to operate one Microsoft product, for example Word, learning how to use another Microsoft product such as Publisher will be easier and take a shorter amount of time [BUIE99].

HCI standards also reduce the number of look and feel decisions that have to be made during design. This helps to speed up the design process.

2.5.2 Contents of an HCI standard

HCI standards include statements about the features of the product's HCI design. These statements are either requirements (the HCI must have some feature if it is to comply with the standard) or recommendations. Most statements are recommendations, as the standard is trying to be general enough to cover a wide variety of applications. There are also very few design features that are always needed. HCI standardisation is not as rigid as, for example, telecommunications standards [BUIE99].

Along with recommendations, a standard usually has the following information [BUIE99]:

- Rationale and principles behind the standard.
- Examples of how the standard might be implemented.
- Possible exceptions to the recommendations.
- References and sources of additional information.

Some standards (normally military or government) include a compliance section. This states the method to be used to check if the HCI complies with the standard.

2.5.3 Types of standards

There are currently a number of different types of standards [BUIE99]:

- International standards which have been developed by organisations to reflect agreements among national members, for example ISO (International Organisation for Standardisation) [ISO04].
- National standards which have been developed by organisations to reflect agreements among companies and other entities within a country, for example ANSI (American National Standards Institute), BSI (British Standards Institution) and the SANS (Standards South Africa) [ANSI04] [BSI04] [SANS04].
- Military and government standards, for example Section 508 of the Disability Act requires that all United States federal agencies' electronic and information technology must be accessible to people with disabilities. This includes ensuring that federal agency web interfaces are available to visually impaired users through

the use of 'screen readers' [BUIE99] [SECT03].

- Company standards which stipulate the look and feel of products that run on a specific platform, for example standards for Microsoft, Macintosh and IBM [ISII02].

- Project standards for a specific project. For example, the Open Source content management system Typo 3 has specific guidelines and standards for developers who add extra modules [SKARH04].

2.5.3.1 Specific standards for HCI and usability

There are a number of different standards which deal with HCI and usability specifically. A few of these standards are [INTE01]:

ISO/IEC 10741-1: Dialogue interaction - Cursor control for text editing. This standard specifies how the cursor should move on the screen in response to the use of cursor control keys.

ISO/IEC 18021: Information technology - User interface for mobile tools. This standard contains user interface specifications for PDAs.

ISO 14915: Software ergonomics for multimedia user interfaces. This standard provides recommendations for multimedia aspects of user interfaces [BUIE01].

ISO 9241: Ergonomic requirements for office work with visual display terminals.

ISO 11581: Icon symbols and functions.

Discussing all of the above standards in detail is beyond the scope of this dissertation. However, two of the standards which have greater relevance to this dissertation are discussed, namely ISO 9241 and ISO 11581:

2.5.3.2 ISO 9241: Ergonomic requirements for office work with visual display terminals

This standard provides detailed guidance on the design of user interfaces. It states requirements and recommendations relating to the hardware, software and environment that contribute to usability. Ergonomic principles are also dealt with [INTE01].

The ISO 9241 standard consists of a number of parts, six of which relate to HCI [ISO9241]:

- Dialogue principles - General principles which apply to the design of dialogues between humans and information systems.
- Presentation of information - Recommendations for presenting information on visual displays.
- User guidance - Recommendations for the design and evaluation of user guidance attributes, e.g. prompts, online help and feedback.
- Menu dialogues - Recommendations for the design of menus.
- Direct manipulation dialogues - Recommendations for the design and manipulation of objects in a graphical user interface.
- Form-filling dialogues - Recommendations for the ergonomic design of form-filling dialogues.

2.5.3.3 ISO/IEC 11581: Icon symbols and functions

This standard specifies the presentation and operation of icons. Five different types of icons are discussed [INTE01]:

- Object icons – e.g. a document or folder icon.
- Pointer icons – e.g. a selection arrow.
- Control icons – e.g. a scroll bar or check box icon.
- Tool icons – e.g. an eraser or pencil icon.
- Action icons – e.g. icons which represent an application.

In the standard the function of each icon is outlined. For example, pointer icons have an indicating, selecting and manipulating function. The pointer icon should indicate to the user and to the system where the next user interaction (e.g. selecting) could take place. The selecting function allows the user to explicitly identify an object or objects which will be the target of subsequent actions. The manipulating function allows the user to further control the objects selected, for example the editing of areas of text and graphics [ISO11581].

Recommendations are also made for some of the 'default' icons, such as a text pointer icon (used by most word processors, figure 2.2) and border control icons (used to resize windows and borders, figure 2.3)

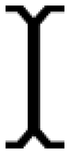


Fig 2.2 Text pointer [ISO11581]

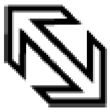


Fig 2.3 Border control icon [ISO11581]

Standards South Africa has adopted ISO 11581 and published a South African version SANS 11581 [SANS11581].

2.5.4 Difficulty in applying standards in HCI

According to Jared Spool, founding principle of the usability consulting firm User Interface Engineering (www.uie.com), standards and guidelines address less than 10% of the questions that arise during user interface design [BUIE01]. This means that even if standards are implemented correctly, a large portion of the usability and interface decisions will still have to be taken by the program designer. The usability of the system is greatly dependent on the HCI skills of the interface designer.

A second difficulty with HCI standards is that an interface which complies with certain standards may lead a customer or client to believe that it is also usable. This may be incorrect, as the product may comply with a standard but not meet the customer's usability needs. Standards tend to cover the features of a product (e.g. what it will look like) but not the usability process. The usability process depends on the nature of the user, task and environment.

A third difficulty with standards is that they take time to be developed and adopted. This poses a problem for the developer, as technology is advancing at a rapid rate. For example, there may be a new type of web interface which a developer wants to implement. However, no usability standards are available for the new interface.

Another weakness with current interface standards is that the topic of security principles has not yet been incorporated into the standards. Guidelines or recommendations are not given in the HCI standards on how an interface can encourage a user to implement good security principles. Standards can, however, be used to help understand the context in which particular attributes may be required. Usable products can be designed by incorporating product features and attributes known to benefit users in a particular context of use.

From this section it is evident that standards are not sufficient on their own. Standards are important, but they have a number of weaknesses. These weaknesses highlight the need for a broader set of criteria which address security issues and can be used alongside standards to ensure the usability of an interface. A possible set of criteria, developed in later chapters to focus on security, is discussed in the next section.

2.6 Criteria for a successful HCI

"There is one answer to every question about user interface design, and that is -- It depends." -- Jim Foley, Mitsubishi Electric Research Laboratory [BUIE00]

The field of HCI has been well researched and principles have been established. The operation of computers has become much easier over the past 20 years. One of the key players in the field of HCI is Jakob Nielsen. He has been involved in HCI and usability for many years and has developed a list of ten criteria for a successful HCI [NIEL02]. These criteria, shown in table 2.1, have been widely accepted and used [NIEL90] [NIEL94].

Table 2.1 HCI criteria

No.	***Criteria***	***Description***
One	*Visibility of system status*	It is important for the user to be able to observe the internal state of the system through the HCI. This can be achieved by the system providing correct feedback within a reasonable time.
Two	*Match between system and the real world*	An HCI which uses real-world metaphors is easier to learn and understand. This will assist a user in figuring out how to successfully perform tasks.
Three	*User control and freedom*	System functions are often chosen by mistake. The user will then need a clearly marked exit path.

No.	Criteria	Description
Four	*Consistency and standards*	Words, situations and actions need to be consistent and mean the same thing. A list of reserved words can assist in this area.
Five	*Error prevention*	It is obviously best to prevent errors in the first place through careful design. However, errors do occur and they need to be handled in the best possible way.
Six	*Recognition rather than recall*	The user should not have to remember information from one session to another. Rather, the user should be able to 'recognise' what is happening.
Seven	*Flexibility and efficiency of use*	The system should be efficient and flexible to use. Productivity should be increased as a user learns a system. The system should not control the user; the user should rather dictate which events will occur. The system should be suitable for new and power users [MICH95].
Eight	*Aesthetic and minimalist design*	Information which is irrelevant should not be displayed. The user should not be bombarded with information and options.
Nine	*Help users recognise, diagnose and recover from errors*	Error messages need to be clear and suggest a solution.
Ten	*Help and documentation*	Users tend to turn to help and documentation as a last resort. Help functionality needs to be context-sensitive and easy to search.

The above criteria are quite comprehensive and are valuable in the analysis and design of a user interface. The criteria focus on the general aspects of an interface. However, security aspects of an interface are not addressed. In order to achieve the goal of this dissertation the above criteria will need to be adapted, refined and added to so as to focus on interfaces found in a security environment. The modified HCI criteria are presented in chapter 4.

In the next section the future trends of the fields of HCI are discussed.

2.7 The future of HCI

The role of technology in users' lives continues to grow. Almost every aspect of a user's life is impacted in some way by technology. Even users in developing countries have access to technology in the form of cell phones. HCI can contribute and facilitate this growth in technology by ensuring the usability of these interfaces. Certain users who would not have been able to operate this technology will be able to do so because of HCI. This means that HCI design guidelines and principles will become more crucial.

The first mainframe computers had very limited interfaces comprising mostly of switches and lights. Interfaces then progressed to text-based command line format interfaces, followed by 2D graphical user interfaces. Technology is now at the point where interfaces are beginning to move into a 3D virtual reality environment. 3D interfaces are already found in computer-aided design, radiation therapy, surgical simulation and data visualisation. As available bandwidth increases, so will the advance of 3D interfaces on the Web. Websites like Nokia.com already use 3D technology to showcase their products. The growth in the use of 3D technology has opened up a new arena for the application of HCI usability and design principles [NOKIA04].

The field of HCI is not limited only to personal computers. PDAs, mobile phones, home entertainment systems, car dashboards and even kitchen appliances can all benefit from the implementation of HCI principles.

The operation of almost any video machine bears testament to the fact that the fields of HCI and usability are not yet fully developed and that HCI principles are not always correctly implemented.

2.8 Conclusion

"If the user can't use it, it doesn't work." -- Susan Dray, Dray and Associates [BUIE00]

In this chapter a brief history of HCI was given, followed by a definition of both HCI and usability, thereby meeting the first objective as stated at the beginning of this chapter. The second objective was met by establishing the current HCI standards. Various criteria developed by Jakob Nielsen were examined, thereby meeting the third objective. The aim of this chapter, namely to provide an overview of HCI, has therefore been achieved.

Many computer monitors around the world have notes stuck on them with instructions on how to do many things (from sending email to creating a spreadsheet). These notes should not be necessary. This shows that not enough attention is being given to HCI. A better understanding of HCI will lead to user interfaces which are easy to learn and intuitive.

The importance of HCI is only going to grow as more people use technology and as technology becomes more and more proliferate. Already users are swamped with interfaces – computers, cell phones, MP3 players. Learning how to operate all these devices off by heart is neither desirable nor feasible. HCI is needed to ensure that these devices remain usable and the operation of them intuitive.

As technology continues to spread, the importance of security is also going to grow. More and more transactions are being conducted electronically and large amounts of personal information are stored in electronic format. Information security is forming a larger part of corporate governance as new legislation is introduced around the world, forcing CEOs to take personal responsibility for the accuracy of financial statements. The processes, controls and information technology behind the generation of companies' financial statements need to be secure [CLARK03].

The security aspects of an HCI are looked at in the next chapter.

Chapter 3
Information Security

3.1 Introduction

The world is moving rapidly into the information age. As this move continues, the value of information increases. Some information's monetary value is priceless, such as personal and private details. Once the security of information has been compromised, it is very difficult and sometimes impossible to re-establish trust. These factors, together with the growth in the Internet, mean that information security is vital [CLARK01].

According to one source [MOBBS02], it is estimated that 75% of information loss or system damage in a company is caused by malicious intent and staff error from within the company. The CSI/FBI Computer Crime and Security Survey found that the likely source of 77% of attacks on a system was disgruntled employees [RICHAR03]. From these statistics it can be seen that external factors such as hackers, crackers and viruses only cause about 25% of the problems. Many security features concentrate on protecting a company from external threats and this leads to a false sense of security, as internal threats are greater [YONA02]. Considerable research has been done into the external factors which influence information security, sometimes to the detriment of solutions to internal factors.

The goal of this dissertation is to see how interfaces can be used to improve the security of a system. Hopefully by improving the interface, fewer mistakes will be made and the user will attempt to bypass fewer security devices. In order to improve an interface in a security environment, a brief overview of information security is needed. The objectives of this chapter are to find a generally accepted definition of information security, identify a framework for security and establish the research that has already been done in this field.

In this chapter a definition of information security along with international standards of information security are given. Existing research in the field of HCI in a security environment is also discussed.

3.2 Definition of information security

Information can be defined as *"knowledge given or received of some fact or circumstance"* [WORLD92] and *"important or useful facts obtained as output from a computer by means of processing input data with a program"* [ANS01]. As described in the definition, information is normally important and useful, which means that it has value. Information can be used to reduce uncertainty about past, present or future events [WIKI03]. The above definition also highlights that information is given and received. The protection of information is therefore important while it is being stored, given and received. The safeguarding of information is made more complex as information is intangible and easily copied. It is also difficult to determine if information has been copied. For example, a sensitive document could have been photocopied or a confidential computer file copied. The document and computer file would normally not provide any evidence to the fact that they have been copied.

Security can be defined as *"freedom from danger, care, or fear"* [WORLD92] and *"the quality or state of being secure"* [MERR03], where secure means *"free from danger, free from risk of loss"* [MERR03].

The combination of the terms 'information' and 'security' leads to 'information security', a term on its own. In literature there are several definitions of information security. This is complicated by the similarity of terms such as 'information security', 'computer security' and 'information technology security'. Information security can be defined as:

"The protection of information systems against unauthorised access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorised users or the provision of service to unauthorised users, including those measures necessary to detect, document, and counter such threats" [PELTI02].

According to the American National Standards Institute, information security is:

"The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional" [ANS01].

As can be seen from these definitions, information security deals with the protection of all information. This information can be in electronic format or stored in a physical paper file. Information security is not synonymous with computer security and information technology security. Computer security and information technology security are a subset of information security and are concerned with the security of all computer systems along with the security of information stored in electronic format. Information security covers not only information, but also the infrastructure that carries, stores or manipulates the information. This infrastructure could be computer programs, hardware and processes [WIKI03a].

For the purposes of this dissertation only information in electronic format is covered. Information security can therefore be defined as: *"The protection of information which is stored and transferred in electronic format from unauthorised access, interception, modification and destruction."*

Now that a definition of information security has been established, in the next section some standards for information security are examined.

3.3 Information security standards

Standards help businesses determine what constitutes good practices in information security. There are several information security standards. Three of these standards are as follows:

- The Forum's Standard of Good Practice - The Standard for Information Security. The Forum's Standard provides a practical statement of good practice for information security aimed at businesses [ISF00].
- ISO 17799 – This standard is the successor to BS 7799. ISO 17799 is "a comprehensive set of controls comprising best practices in information security" [ISO]. This standard has been accepted by the Information Security Institute of South Africa [ISIZA00].
- ISO 7498-2 – Published in 1989, this standard provides a high level model to address information security.

Many companies have also developed their own internal standards. The standard that a company chooses to follow depends on its circumstances and whether or not the company wishes to receive some form of certification of compliance, for example to become a certified ISO 17799 compliant company.

Certification is important because some companies will only do business with other companies that have a certain certification. Certification also gives a company a competitive edge over companies that are not certified.

Businesses are also moving into an environment in which executives of a company are responsible for both a company's assets and its intellectual property. In order to protect themselves, companies need to prove that they have adequate security measures in place [KING03]. Legislation such as the Electronic Communications and Transactions (ECT) Act also provides a legal motivation for companies to implement security standards [ECTACT02].

The information security standard discussed and used in this dissertation is the ISO standard 7498-2. This standard was chosen because it approaches information from a non-technical, top-down approach, unlike other standards which focus on technical details.

According to ISO standard 7498-2, the protection of information can be addressed in terms of the five security services [YASK] shown in figure 3.1.

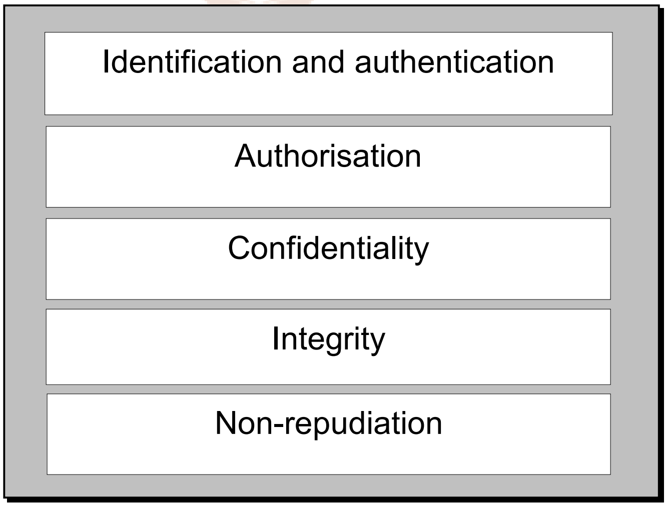


Fig 3.1 Security services

The aim of these services is to aid the user by ensuring that sensitive information is protected and secure. In the next section these five services are elaborated on and examples given of how they relate to HCI.

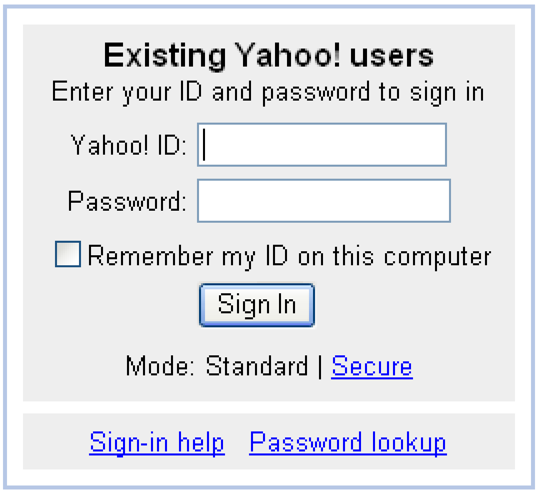
3.4 Information security (IS) services

Information security comprises five services: identification and authentication; authorisation; confidentiality; integrity and non-repudiation.

3.4.1 Identification and authentication

Identification and authentication is the first step to protecting information. A user needs to be identified first, for example by a username. The user then needs to be authenticated to see if they are who they say they are. There are different ways of authenticating a user – by what they know (e.g. a password), by what they have (e.g. a smart card) and by who they are (e.g. biometrics) [VONS97].

With regard to HCI, a login window asking for a username and password can be used to implement the graphical aspect of identification and authentication (figure 3.2).



Existing Yahoo! users

Enter your ID and password to sign in

Yahoo! ID:

Password:

□ Remember my ID on this computer

Mode: Standard | Secure

Fig 3.2 Example of login in Yahoo! mail

Other technologies, apart from a username and password, are also used for authentication. An example of this is fingerprint scanning in the field of biometrics. In cases like this it is important for the interface to guide the user as to how to use the technology, since it is potentially a new technology to the user, one which they do not yet know how to operate.

One of the main problems a user experiences with identification and authentication is that they forget their username and password. Yahoo! mail attempts to solve this problem by providing an option in the interface to remember the user's ID (username). Some interfaces also offer to remember a user's password. A password lookup service via the

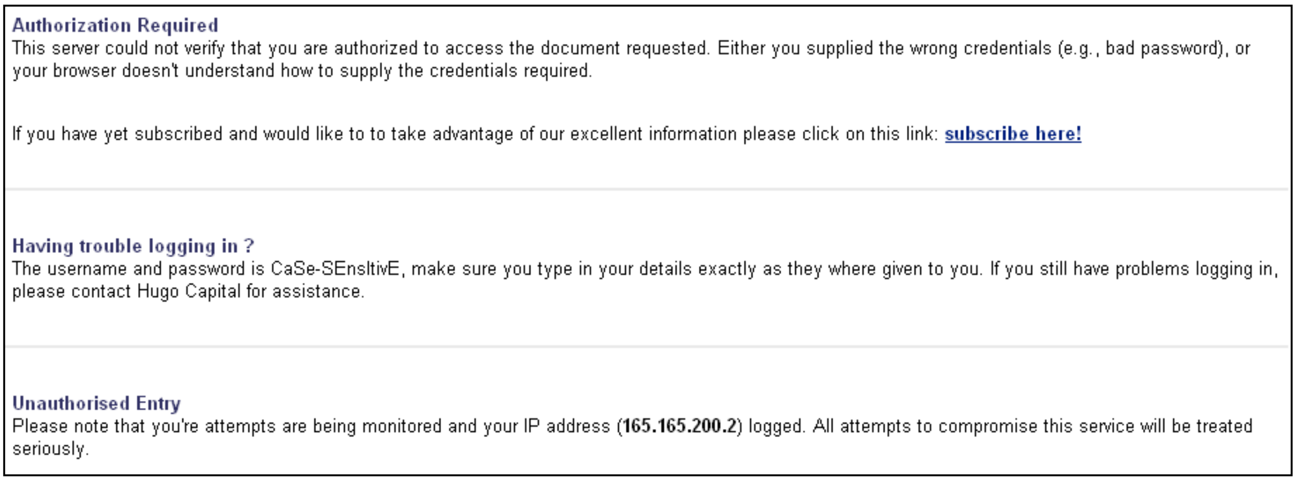
'Password lookup' link is also provided. A password lookup service verifies a user by confirming personal information which the user provided when they registered. Correct answers to all the questions results in the user's password being reset.

3.4.2 Authorisation

The next step towards enforcing IS involves determining whether or not the authenticated user has the right to access the computer system or information requested. This could be done by checking the username against a database. A system may use mandatory access control or discretionary access control. Mandatory access control is where all computer programs, databases and workstations are protected by default. A security policy will determine the level of the protection. Discretionary access control, on the other hand, is where the user who created the information determines the level of protection [VONS97].

The service of authorisation is not directly addressed by HCI. However, the aim is to make identification, authentication and authorisation as easy as possible for a legitimate user so that they do not try to bypass these services. For example, if a password is too complicated to remember, or if there are too many passwords, a user may just ask a colleague for their password. In this example the password is being authorised and not the user. This creates a security issue as a password is used to uniquely identify a user.

Figure 3.3 shows an example of an error message of a failed authorisation attempt. Error messages should be user-friendly and explain a possible solution. This message also logs the user’s IP address and warns them against trying to compromise the security of the website.



Authorization Required
This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password), or your browser doesn't understand how to supply the credentials required.

If you have yet subscribed and would like to to take advantage of our excellent information please click on this link: **subscribe here!**

Having trouble logging in ?
The username and password is CaSe-SEnsItivE, make sure you type in your details exactly as they where given to you. If you still have problems logging in, please contact Hugo Capital for assistance.

Unauthorised Entry
Please note that you're attempts are being monitored and your IP address (**165.165.200.2**) logged. All attempts to compromise this service will be treated seriously.

Fig 3.3 Incorrect username or password (HugoCapital.com)

A possible problem a user faces with authorisation is when they are refused access to certain content to which they think they should have had access. A message which describes why they were refused access to certain material will hopefully relieve the user's frustration. The steps that need to be taken by the user to gain access should also be listed.

3.4.3 Confidentiality

Confidentiality is the service that protects data from being revealed to unauthorised users. Technologies such as public key encryption and private key encryption ensure confidentiality. Secure socket layers (SSL) is an example of private key encryption.

A large majority of computer users do not understand encryption, which means that they probably do not trust it and will therefore be reluctant to use it. HCI's goal in this situation would be to simplify the encryption process and to reassure the user that the transaction they are undertaking is safe.

As can be seen in figure 3.4, Internet Explorer attempts to do this by showing the 'padlock' icon when encryption is taking place.

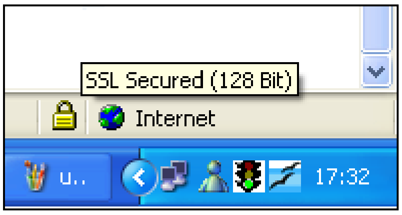


Fig 3.4 Padlock in Internet Explorer conveying that SSL is being used

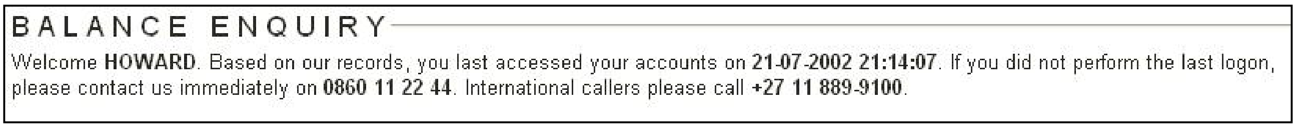
Many users do not understand the technology which enforces confidentiality. This means that they are unlikely to trust the system, and if a user does not trust a feature, they will not use it. This can be seen by users who do not purchase goods online because of security fears.

3.4.4 Integrity

Not only should the information be kept confidential, but the integrity of the information should also be guaranteed. Only authorised users should be allowed to modify information.

Some of the technologies which implement integrity are checksums and hash-functions. A checksum uses a secret key to calculate a value from the information. A hash-function is similar to a checksum, but does not normally use a key. Instead, the hash-function uses an algorithm which calculates a value based on the information [VONS97a].

The interface needs to convey the service of integrity to the user. This can be accomplished through a message which reassures a user that the information has not been tampered with.



BALANCE ENQUIRY

Welcome **HOWARD**. Based on our records, you last accessed your accounts on **21-07-2002 21:14:07**. If you did not perform the last logon, please contact us immediately on **0860 11 22 44**. International callers please call **+27 11 889-9100**.

For example, figure 3.5 shows a message that appears when a user logs in to a banking site.

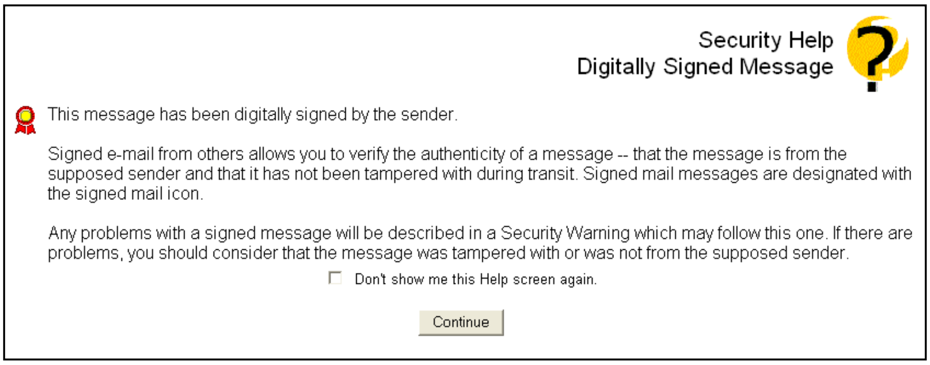
Fig 3.5 The interface of a banking website which promotes integrity

It states the time and date of the last login of the user. The user is then reassured that no one has accessed their account since they last logged in. This helps the user feel more confident and secure.

3.4.5 Non-repudiation

The last step towards enforcing information security is to ensure accountability. If a user changes information, they should not be able to deny it at a later stage. Public key encryption is used in non-repudiation [VONS97].

Figure 3.6 shows an example of how non-repudiation can be enforced. The email has been digitally signed, which means the sender of the email cannot later deny sending the email. The digital signature also validates to the receiver the identity of the sender.



Security Help
Digitally Signed Message

This message has been digitally signed by the sender.

Signed e-mail from others allows you to verify the authenticity of a message -- that the message is from the supposed sender and that it has not been tampered with during transit. Signed mail messages are designated with the signed mail icon.

Any problems with a signed message will be described in a Security Warning which may follow this one. If there are problems, you should consider that the message was tampered with or was not from the supposed sender.

□ Don't show me this Help screen again.

Fig 3.6 Digitally signed message

A digital signature works by a user signing a message with their private key to which only they have access. When a user receives a digitally signed message, they use the sender's public key, which is freely distributed, to verify the signature [VONS97].

A typical problem with enforcing non-repudiation which users experience is that they do not keep their private keys secure. Once a private key has been imported into an email program, any person who has access to the user's computer can send a potentially fraudulent email. The interface needs to inform the user that a digital signature only works if their private key is secure.

In the next section HCI and security are looked at.

3.5 HCI and security

Extensive research has been done in the field of HCI. Many articles and papers have been published by usability experts such as Jakob Nielsen, Donald Norman and Bruce Tognazzini [HUMA03] [TOGNA] [NORMAN] [NIELSEN].

An extensive amount of research has also been done in the various fields of security: computer security, information security, web security and others [FIRST]. As can be seen, both HCI and security are well established fields, but not much research has been done into the combined field of HCI and security. Very little exists in terms of literature in the field of HCI in a security environment. Two articles that have been identified as being similar to this dissertation are:

- Usability of Security: A Case Study 1998 (Alma Whitten, Carnegie Mellon University and J.D. Tygar, University of California). In this paper an introduction is given to usability and security. This is followed by a case study of PGP. PGP was chosen because the authors wanted to see if a person who was not familiar with security was able to operate a security program [WHIT98].
- User Interaction Design for Secure Systems (Ka-Ping Yee, University of California, Berkeley). In this paper ten design principles for an interface are given. The idea behind these design principles is that violating one of them will lead to a security vulnerability [KAPIN02].

It is clear from the lack of literature that the HCI aspect of security has been neglected. There is therefore a need for more research into the field of HCI in a security environment, and hence the motivation for this dissertation.

3.6 Conclusion

In this chapter a definition of information, security and information security was given. International standards for information security were then discussed, followed by an overview of the information security services from an HCI perspective. Previous research into the field of HCI in security was examined.

Based on the different definitions of information security, a definition for the purposes of this dissertation has been established. The first objective of this chapter has therefore been achieved. The second objective of identifying a framework has been met by introducing the information security services from ISO standard 7498-2. The last objective has been accomplished through the discussion on previous research. The goal of this chapter, which was to provide an overview of information security, has therefore been achieved.

In later chapters it is shown how the interface of a system can help to enforce and implement the IS services. In the next chapter interfaces in a security environment are discussed. .

Chapter 4
Security HCI (HCI-S)

4.1 Introduction

"I think that the seemingly different aims of HCI and security (HCI tries to make things easy, while some people construe information security to make things difficult) is a very nice topic for further investigation. The "making things difficult" aspect of computer security is primarily aimed at confidentiality issues - whereas HCI research relates much better to the availability aspect of information security - it in my opinion is also assisting with integrity (doing things easier makes it less likely that we make mistakes...)" - Reinhard Botha [BOTH02].

The assumption is sometimes made that improving security limits usability. Often the opposite is true: improving usability improves security. A user is more likely to implement the security services discussed in chapter 3 if it is easy to do so. Many current security systems are too confusing and difficult for the average user to implement. Security may not be a priority for a user, which means they are unlikely to try to figure out a way to implement a security function. The user may not be aware of the correct way to complete a task and may need to be guided by the interface. Users also tend to choose the path of least resistance. This can sometimes work against security measures [YEE02].

This leads to the security of a system being only as good as its interface [JEND00]. In order to improve the interface, and hence the security of a system, which is the goal of this dissertation, the HCI criteria discussed in chapter 2 need to be adapted to focus on security issues. The aim of this chapter is therefore to develop HCI-S (human computer interaction – security) criteria so that they can be used in future chapters to analyse existing interfaces. The first objective of this chapter is to introduce a new term – HCI-S. HCI-S is not found in any other literature and a definition will therefore need to be established. The second objective of this chapter is to define the HCI-S criteria so they can be used by developers to design better security interfaces. The introduction of the HCI-S criteria is also important in that they can be used to evaluate existing interfaces from a security point of view.

In this chapter the concept of a security HCI (HCI-S) is developed. It will then be seen how these criteria relate to trust. This is followed by a discussion of various HCI-S criteria.

4.2 Definition of a security HCI (HCI-S)

The objective of this dissertation is to see how the security of a system can be improved by improving the interface. In order to achieve this objective a new term, HCI-S, is introduced.

Reference to HCI-S has not been found in current literature. Therefore for this dissertation security HCI (HCI-S) can be defined as *the part of a user interface which is responsible for establishing the common ground between a user and the security features of a system. HCI-S is human computer interaction applied in the area of computer security.*

HCI-S deals with how the security features of a graphical user interface can be made as user-friendly and intuitive as possible. The easier a system is to use, the less likely the user will make a mistake or try to bypass the security feature. This adds to the integrity of a system. HCI-S's goal is to improve the interface in order to improve the security. This leads to the system becoming more secure, robust and reliable.

HCI's focus is on making a computer system as easy to use as possible. On the other hand, it is sometimes perceived that security features make a system harder to use. HCI-S addresses this issue and strikes a balance between security and ease of use.

HCI is a broad field which encompasses all forms of interaction between users and computers. HCI-S, on the other hand, is more focused and only concentrates on the security features of an interface.

For the HCI criteria mentioned in chapter 2 to be relevant for this dissertation, they need to be adapted to the HCI-S criteria.

4.3 Criteria for a successful HCI applied in the area of security

The new criteria are called HCI-S criteria and are listed in table 4.1. Figure 4.1 shows how these HCI-S criteria relate to the standard HCI criteria.

Table 4.1 Summary of HCI-S criteria

No.	***Criteria***	***Description***
1	*Convey features*	The interface needs to convey the available security features to the user.
2	*Visibility of system status*	It is important for the user to be able to observe the security level of the internal operations of a computer system.
3	*Learnability*	The interface needs to be as non-threatening and easy to learn as possible.
4	*Aesthetic and minimalist design*	Only relevant security information should be displayed.
5	*Errors*	It is important for the error message to be detailed and to state, if necessary, where to obtain help.
6	*Satisfaction*	Does the interface aid the user in having a satisfactory experience with a system?
Does the interface lead to trust being developed?		
	Trust	It is essential for the user to trust the system. This is particularly important in a security environment.

The reason for these criteria is to assist in the development and design of interfaces which are used in a security environment. As was seen in chapter 3, information security is critically important and there is a need for criteria that can be used to ensure that the interface is not a 'weak' point in a system's security. These criteria are based on Nielsen's HCI criteria discussed in chapter 2 [NIEL02]. They have been modified and condensed to only the essentials in a security environment.

Figure 4.1 shows a comparison between the existing HCI criteria and the proposed HCI-S criteria. Criteria in the blue circle from part of HCI, while the criteria in the brown circle are the HCI-S criteria. As can be seen from the diagram, three criteria overlap and form part of both HCI and HCI-S. The criterion of *Learnability* has been formed from three existing HCI criteria. Two new criteria – *Satisfaction* and *Convey Features* are added.

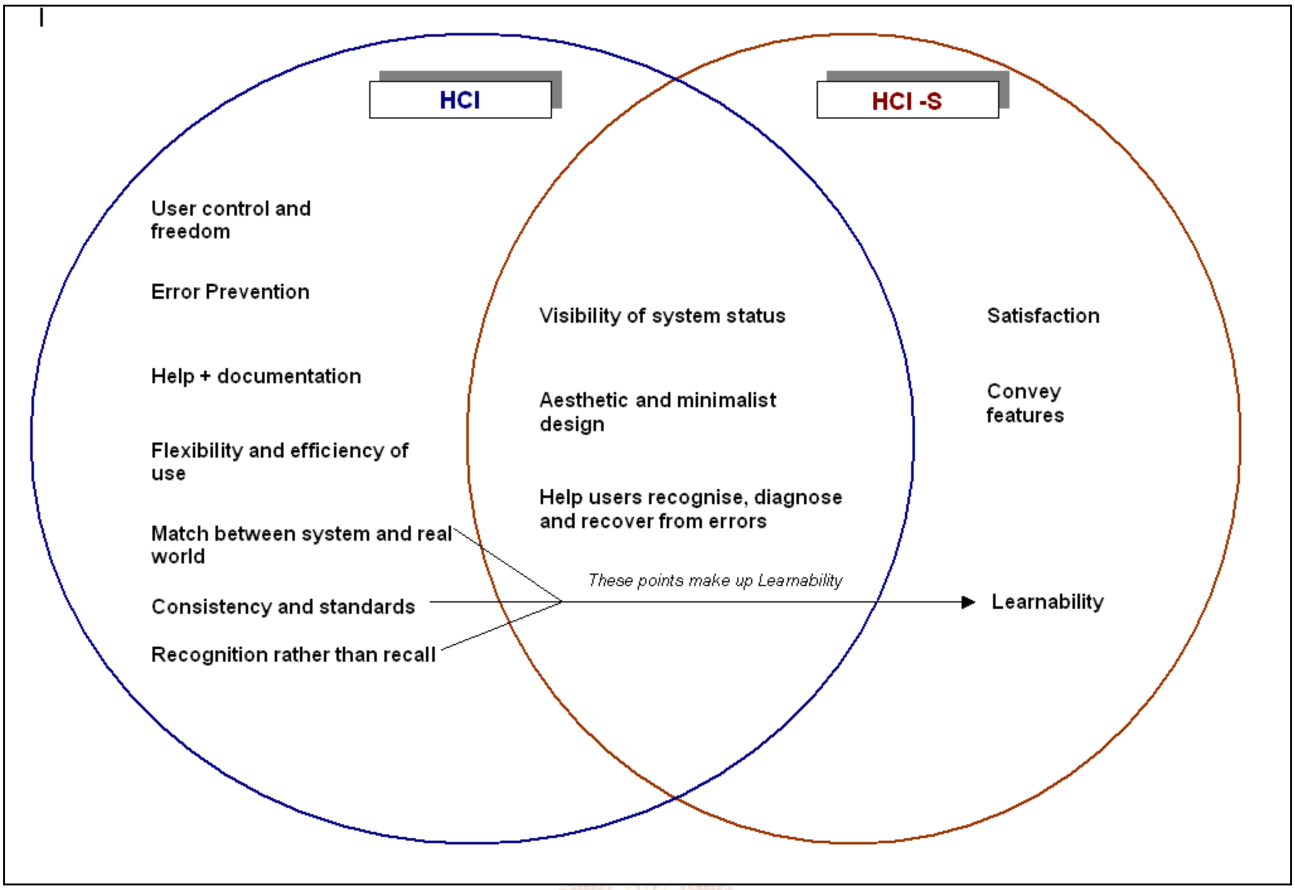

HCI
HCI -S
User control and freedom
Error Prevention
Help + documentation
Flexibility and efficiency of use
Match between system and real world
Consistency and standards
Recognition rather than recall
Visibility of system status
Aesthetic and minimalist design
Help users recognise, diagnose and recover from errors
These points make up Learnability
Satisfaction
Convey features
Learnability

Fig 4.1 Comparison between HCI and HCI-S

In the next paragraphs each HCI-S criterion is discussed in more detail.

4.3.1 Visibility of system status

Visibility of system status allows the user to observe the internal state of the system. An example of this is the small padlock which is displayed in the bottom right-hand corner of Internet Explorer when viewing a secure web page. The padlock informs the user of the status of the web page and that encryption is being used.

4.3.2 Aesthetic and minimalist design

A balance needs to be struck by providing enough information for a first-time user while at the same time not providing too much information for an experienced user. Irrelevant information should not be displayed. The user should not be bombarded with information and options. As far as possible, technical terms should be avoided.

If the interface to a security function looks too complicated or confusing, the user may not feel confident enough to use it. A minimalist design can address this situation.

4.3.3 Help users recognise, diagnose and recover from errors

Errors which occur when dealing with a security function have the potential to be more lethal than normal errors. For example, take the situation of an error occurring in the middle of a banking transaction and the following error message being displayed: "Your interactive session is no longer active" [FIRST02]. This error message is confusing and may cause a user to feel concerned about the outcome of the transaction. It is important for the error message rather to be detailed, specific and to state what action needs to be taken and how to obtain additional assistance. A generic message for all errors is not adequate.

4.3.4 Learnability

When developing HCI-Ss in a software environment it is necessary to be more detailed; hence the three similar HCI criteria of *Match between system and real world, Consistency and standards,* and *Recognition rather than recall.* The three HCI criteria are three aspects of the same principle. In this dissertation it is not necessary to explore each in detail and they have therefore been combined into the one HCI-S criterion of *Learnability*.

Security is often not a priority for a user, even though it is very important. It is easy for a user to put off learning about security. Therefore it is essential for a security HCI to be as user-friendly and as easy to learn as possible. A casual user who has not used the software for a while should not have to learn everything over again [MICH95].

An interface which uses real-world metaphors is easier to learn and understand. For example, items such as keys and padlocks have real-world uses and meanings. These items and their meanings can be transported and used in an interface. A user who then sees these items will recognise them and have an idea of what they could be used for in the interface. This will assist a user in determining how to perform tasks successfully.

An interface which is consistent and based on standards is also easier to learn. Many users are familiar with the conventions of interfaces used in the Microsoft Windows environment. Icons, windows and menus all behave the same in the Windows environment, which means it is easier for a user to learn a new program based on these standards. When it comes to security features in an interface, there are certain conventions which are used frequently. For example, usernames and passwords are security features which are often used. The user may become confused if different terminology is used for usernames and passwords, for example 'profile' instead of 'username' and 'access code' instead of 'password'. It is therefore advisable for an interface to be consistent and adhere to standards.

If security features are irritating, then the user's satisfaction will be low. However, a security feature which is easy to use and works correctly will lead to a high level of satisfaction. The security feature could be a firewall which has just prevented illegal access to the user's hard drive or login page on a website.

4.3.5 Satisfaction

The criterion of *Satisfaction* is concerned with the level of enjoyment a user experiences while using the interface of an application. This is important in a security environment as security is usually not a primary activity for computer users. A user’s experience with security features needs to be pleasant and satisfying otherwise they may neglect the security of their system due to a lack of *Satisfaction*. For example, if it is too much effort for a user to encrypt a sensitive document, they may take a chance and email the document unencrypted. *Satisfaction* is a new criterion which is added to the other HCI-S criteria.

4.3.6 Convey features

The interface should inform the user in a clear manner of the available security features. For example, the security features of integrity and confidentiality are available on most e-commerce websites. One of the ways in which these features is implemented is through SSL. The use of SSL by a website should be conveyed to the user by the interface along with the purpose and benefits of SSL.

The use of pictures can be an effective way of conveying features, especially for a user who is not technically minded. Figure 4.2 shows an example of a graphic which could depict the feature of encryption.

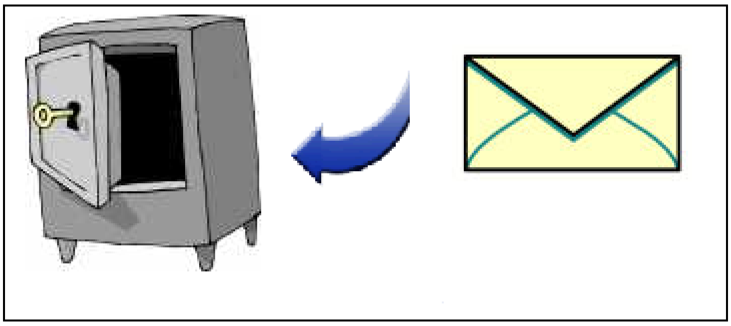


Fig 4.2 Encryption [ENVE] [SAFE] [ARRO]

The HCI-S criterion of *Convey features* informs the user of the available security features, while the criterion of *Visibility of system status* allows the user to 'see' if these features are active and being used. *Convey features* is also a new criterion.

The result of applying the six HCI-S criteria is trust, which is discussed in the next paragraph.

4.4 The HCI-S criteria lead to trust

The successful implementation of all of the above criteria will lead to trust. Trust is important because if a person is to use a system to its full potential, be it an e-commerce site or a computer program, it is essential for them to trust the system.

According to the Oxford Dictionary, trust can be defined as *"The belief or willingness to believe that one can rely on the goodness, strength, ability of somebody or something"* [OXFO95]. This definition can be adapted for the HCI-S criterion of *Trust* to *the belief or willingness to believe, of a user, in the security of a computer system*. The degree of trust a user has in a system will determine how they use it. For example, a user who does not trust a website will not supply their credit card details.

The interface plays an important role in fostering trust between the system and user. One way this can be done is by the interface informing the user in a clear manner of the risks and how these risks can be minimised.

When a person walks into a physical shop they decide whether or not they will trust the business based largely on what they can see. In the same way, users often make a decision regarding trust based on what the interface tells them and what it looks like. A high quality interface which projects quality and professionalism will also foster trust. This may be a false sense of trust if the technology behind the interface is not adequate.

The amount of trust an interface needs to develop with a user depends on the purpose of the system. If the system is an e-commerce site, then enough trust needs to be fostered for the user to hand over their credit card details.

As the Internet continues to grow, its success will depend on gaining and maintaining the trust of visitors. Trust on the Internet is not based solely on technical security features, but also on the user's feeling of control of the interactive system [DHER00].

Research done by InteractionArchitect.com [DHER00] points to six primary factors which convey trust:

1. ***Fulfilment.*** This is the process the user works through from the time of purchase to delivery. Here it is important that the website clearly indicate how orders will be processed and provide information on how to handle problems. If a transaction is not completed satisfactorily, the customer needs to be told what recourse they can take. It is also important to inform the user of the privacy policy regarding personal information. Overall, the simpler it is for a user to buy a product, the better.
2. ***Technology.*** This is the way in which the website functions technically. Does it use technologies such as SSL and digital certificates in order to keep transactions secure? Does the site load quickly and function adequately? A website which does not display correctly or has errors on it will not foster trust.
3. ***Seals of approval***. These are symbols, like VeriSign, TRUSTe and Visa, which are designed to reassure the visitor that security has been implemented according to a certain standard on the computer network as a whole.
4. ***Presentation***. A professionally designed site is more likely to foster trust. This can also be seen in the brick and mortar world where a business which is professional and has a neat and tidy appearance is more likely to be trusted by its customers.
5. ***Navigation***. This is the ease of finding what the user is looking for. Is the navigation predictable and content easy to find? Prompts, guides, tutorials and instructions can aid the user in performing transactions.
6. ***Brand***. The brand reflects the company's reputation. A well known brand which has a reputation of being trustworthy in an off-line environment is likely to foster trust online [DHER00].

The above factors are important because five of them relate directly to HCI-S – seals of approval, navigation, fulfilment, presentation and technology [DHER00]. This relationship is illustrated in figure 4.3.

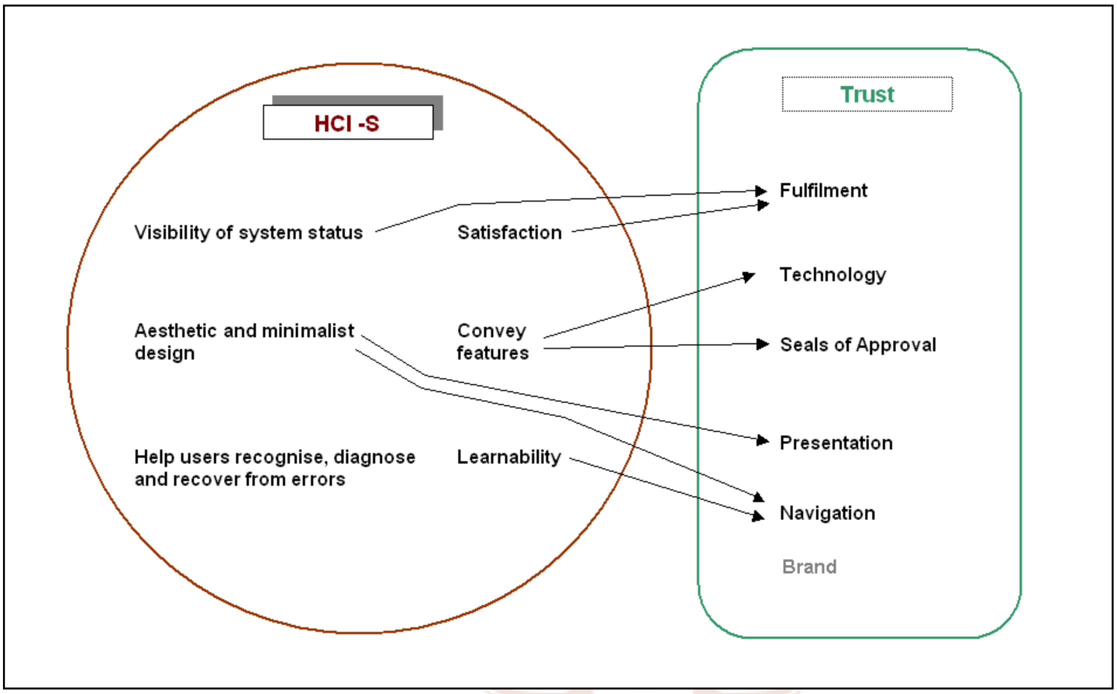


Fig 4.3 Trust related to other HCI-S criteria

The six factors which relate to trust (shown in the green block in figure 4.3) can be applied to security in the following way:

- ***Fulfilment***. Here the HCI-S criteria of *Convey features* and *Visibility of system status* are important. The user needs to know what security features are available and be clearly informed when these features are being used. Fulfilment should lead to *Satisfaction.*
- ***Technology***. HCI-S is not concerned with the technical aspects of security. However, it is responsible for *Conveying* these *features* to the user. When a feature, for example SSL, is being used, the interface needs to inform the user of the *Status* of the active feature.
- ***Seals of approval***. Seals of approval need to be in prominent positions. It is also important for their meaning to be conveyed to the user. Seals of approval would come under the HCI-S criterion of *Convey features.* These seals are third-party endorsements which should help to foster trust between the user and the website.
- ***Presentation***. *Aesthetic and minimalist design* is important in the presentation of a website. The result of an *Aesthetic and minimalist* website is that it is easier to

navigate and use than a cluttered website. This will lead to a more satisfying online experience for the user.

- ***Navigation***. An *Aesthetic and minimalist design* aids navigation. A site which is easy to learn (*Learnability*) is also easy to navigate.

In chapter 7 it is shown how the factor of ‘brand’ assists in the development of trust in an online environment. From the above bullet points it can be seen that these factors overlap with some of the other HCI-S criteria. This means that by applying the HCI-S criteria of *Visibility of system status, Satisfaction, Aesthetic and minimalist design, Learnability* and *Convey features*, *Trust* can be developed.

4.5 Conclusion

In this chapter a definition of HCI-S was given and the HCI-S criteria were introduced and discussed. It was illustrated how the application of the HCI-S criteria leads to the formation of trust. The reasoning behind the HCI-S criteria is to develop a user-centred benchmark for evaluating existing security interfaces and to assist in the design of future interfaces.

By providing a definition the first objective of this chapter has been achieved and the second objective was met by introducing the HCI-S criteria. The goal of this chapter, which was to develop criteria, has therefore been met.

The value of this chapter is that six core criteria have been presented which focus on the implementation of interfaces in a security environment. These criteria can be used to develop interfaces which help to improve the security of an application.

In the coming chapters various interfaces in security environments are analysed according to HCI-S criteria.

Chapter 5
Critical Analysis of Windows XP's Internet Connection Firewall

5.1 Introduction

The growth of the Internet has been explosive. As of June 2004 over 700 million people worldwide use the Internet [GROW04]. Radio took 38 years to reach 50 million customers, TV took 13 years and the personal computer 16 years. The Internet took only 5 years to reach this number [EMIR00]. The popularity of broadband is now making it possible for many home and business users to be connected to the Internet 24 hours a day. In August 2003 there were 4 000 ADSL users in South Africa [WARW03]. South Africa is currently lagging behind other countries such as America when it comes to bandwidth. However, the number of bandwidth connections in South Africa is increasing at a rapid rate. According to Telkom (the supplier of ADSL), demand for ADSL is exceeding supply [STEV03].

The growth of the Internet has also led to an increase in viruses, trojan horses and hacking activity. Clients of a large South African bank, ABSA, were defrauded of over R500 000 during 2003. The clients opened an email attachment which contained 'spyware'. The spyware software logged the users' keystrokes, tracking their usernames and passwords. This information was then emailed back to the hacker. The information was used by the hacker to gain illegal access to the clients' Internet banking accounts [CHARL03]. Correctly installed anti-virus software and a personal firewall could have prevented this. Computers which have always-on broadband connections are particularly vulnerable to hackers.

Unconfirmed reports [GREEN03] suggest that the spyware used in the ABSA case was eBlaster. eBlaster is designed by SpecterSoft and is aimed at parents who want to monitor their children's online activity and at employers who use it to track their employees' actions. The information eBlaster collects, such as keystrokes, is recorded in a log file on the infected computer and can also be sent to a defined email address. Windows XP's Internet Connection Firewall would not have protected a user from eBlaster. This is because XP's firewall does not perform any outbound filtering. This means that trojans and other malicious code on a user's computer are able to “phone home” [WONG02]. XP's Internet Connection Firewall can, however, protect a user's computer from most attacks which originate from the Internet. For example, a hacker who attempts to scan a user's computer for open ports will come up empty-handed if the Internet Connection Firewall is activated.

In the past hackers needed detailed knowledge of computers, networks and protocols. However, today many 'tools' are available on the Internet which make it easier for novice hackers to gain access. Studies show that networks are frequently scanned for weaknesses by hackers. Attacks are only likely to increase as more people connect to the Internet. Microsoft is aware of this and has decided to incorporate a firewall in its latest operating system – Windows XP [MICRO01].

The goal of this chapter is to use the HCI-S criteria suggested in chapter 4 to critically analyse Microsoft Windows XP's Internet Connection Firewall (ICF). The purpose of this is to see how the six HCI-S criteria can be applied in a real-world context. The first objective of this chapter is to examine the ICF interface during activation, configuration and operation so that it can be analysed according to HCI-S criteria. Following from the examination of the ICF, the second objective is then to draw conclusions based on the HCI-S criteria to form a base from which recommendations can be made in the following chapter. The third objective is to identify the advantages and disadvantages of using the HCI-S criteria in order to determine the completeness of the HCI-S criteria. The technical aspects of the ICF will not be analysed, as internal technical workings of applications fall beyond the scope of this dissertation.

Background information is given on Windows XP's firewall, followed by a brief recap of the criteria for a successful HCI-S. The remainder of the chapter deals with the activation, configuration and operation of the firewall from an HCI point of view. The chapter concludes with the advantages and disadvantages of the six HCI-S criteria.

5.2 Background to Windows XP's Internet Connection Firewall

Microsoft has decided to incorporate a firewall called the Internet Connection Firewall (ICF) in its operating system - Windows XP. The ICF comes standard with both the home and professional versions of Windows XP.

The ICF is aimed at home and small office computer users [COLL02]. Its goal is to provide a baseline intrusion prevention device in Windows XP. The ICF will hopefully protect against scans for information and block unwanted inbound packets [MICRO01]. It is a stateful firewall, which means it only allows incoming packets if they are part of a session originating in the XP computer. Any 'rogue' packets are dropped and optionally logged. The ICF can be activated on any network connection, for example an Internet connection or a local network connection.

The reason why the Windows XP ICF has been chosen for analysis in this dissertation is that according to WebSideStory, Windows XP as of May 2003 is used by more than a third of all Internet users [WEBSI03]. The next most popular operating system is Windows 98 with a 25% market share [WEBSI03]. This means that there are millions of users around the world who have the ICF installed on their computers. Many of these users would never have specifically bought and installed a firewall on their computers. They do, however, now have access to a firewall. The usability of the ICF interface therefore has the potential to play a huge role in the security of many computers.

Firewalls have generally been difficult for the average user to set up. Microsoft has attempted to make the ICF a simple and unobtrusive security experience.

In the following paragraphs parts of the interface of the ICF are analysed according the HCI-S criteria.

5.3 Brief recap of criteria for analysis

The following criteria are used to analyse the HCI-S of the ICF:

Table 5.1 Summary of HCI-S criteria

No.	***Criteria***
1	*Convey features*
2	*Visibility of system status*
3	*Learnability*
4	*Aesthetic and minimalist design*
5	*Errors*
6	*Satisfaction*
Does the interface lead to trust being developed?	

No.	***Criteria***
	Trust

Three parts of the ICF are looked at: firstly the activation process, secondly the configuration of the ICF and thirdly the operation of the ICF.

5.4 Activation of the ICF

The installation procedure of an application which has a security function, such as a firewall, is extremely important. If the user perceives the application as being non–essential, then they are less likely to use it. This is especially true if the application is too difficult to install or configure. The ICF is automatically installed on a computer when Windows XP is installed. It still, however, needs to be activated on any new network connections which are created. There are various ways to activate the ICF:

Welcome to Windows Wizard

This Wizard is first seen when Windows XP is installed and guides the user through connecting to the Internet, activating Windows and creating user accounts on a stand-alone computer (not on a network). The ICF will be activated if a connection to the Internet is established [MICRO01].

Network Setup Wizard (NSW)

The NSW presents to the user five options to connect to the Internet. If the user selects an option stating that the PC is directly connected to the Internet, then the ICF will be enabled on the Internet connection [MICRO01].

New Connection Wizard (NCW)

When the NCW is run and 'Connect to the Internet' is selected, the ICF will be enabled on the new Internet connection [MICRO01].

Network Connections folder

The ICF can be enabled by clicking the 'Advanced' tab of the 'Properties' page for a network connection. The Network Connections folder is located in the 'Network and Internet Connections' area of the Control Panel [MICRO01].

As can be seen from the above points, there are a number of ways to activate the ICF. However, from an HCI-S perspective the importance of the ICF is not highlighted in any of the above procedures. This means that the HCI-S criterion of *Visibility of system status* is not adequately met. Many users will not be aware that they have a firewall available on their system.

The following paragraphs describe the process of setting up a new Internet connection using the NCW. It is redundant to analyse all of the activation methods, as they are similar. The NCW is analysed from an HCI-S point of view.

In this example the user does not have any Internet connections yet. So the first step is to click 'Start', then 'Connect To' is followed by 'Show all connections' (figure 5.1).

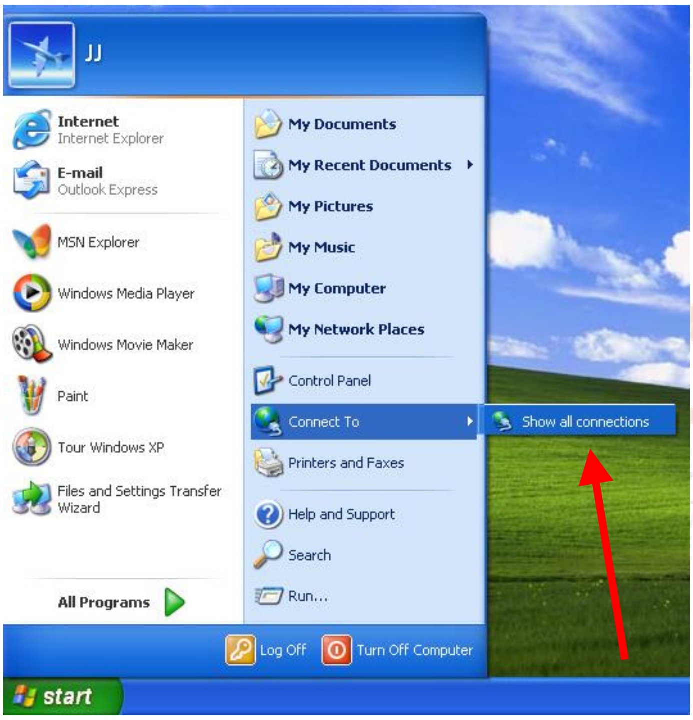


Fig 5.1 Selecting 'Show all connections'

These steps follow the standard Windows format with which many users are familiar.

Security is not mentioned in any way on the start menu (figure 5.1). As was discussed in previous chapters, security is not a priority for many users and they are therefore unlikely to go searching for security functions. If they do decide to look for the ICF, then it may be difficult to find. A 'Security Features' menu option on the Start bar could solve this problem. This would also aid the user if they were looking for options dealing with the general security of their computer. This could be particularly true in the case of ABSA clients who have heard about the spyware software in the press and are now looking for ways to safeguard their computers.

Clicking on the 'Show all connections' option in figure 5.1 will cause the window in figure 5.2 to be shown.

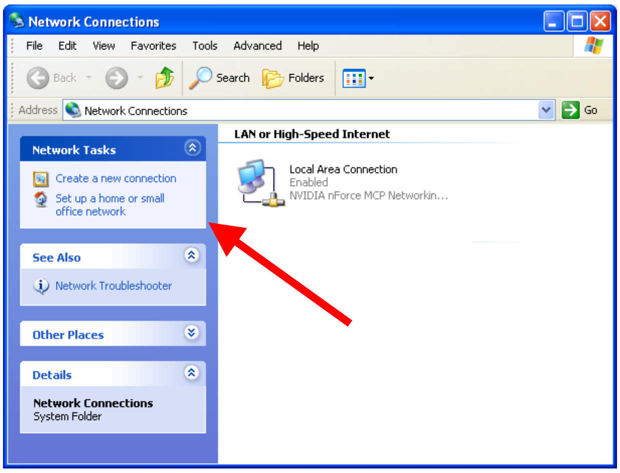
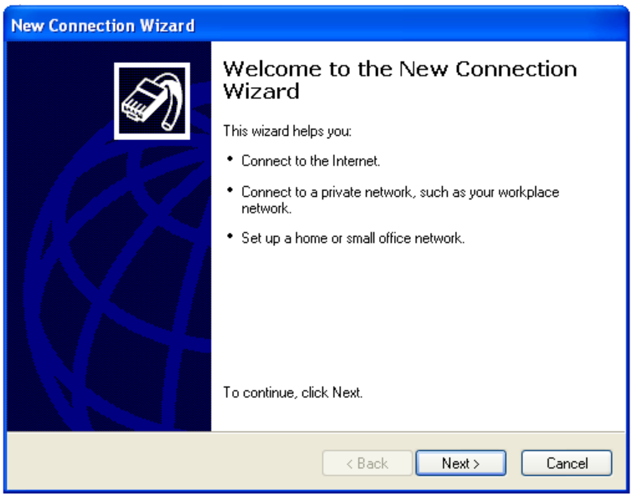


Fig 5.2 Network Connections

The 'Network Connections' window is displayed. The window has a clean and neat layout. It has an *Aesthetic and minimalist design.*

When it comes to creating a new connection, the process has been intuitive. However, there is still at this point no mention of any security features. The user is aware that they are creating a new connection, but they do not know that the ICF can also be activated. The 'See Also' menu on the left has a link to 'Network Troubleshooter'. A link could have been included for more details on security and the ICF.

'Create a new connection' is then clicked, which generates the window in figure 5.3.



Welcome to the New Connection Wizard

This wizard helps you:

- Connect to the Internet.
- Connect to a private network, such as your workplace network.
- Set up a home or small office network.

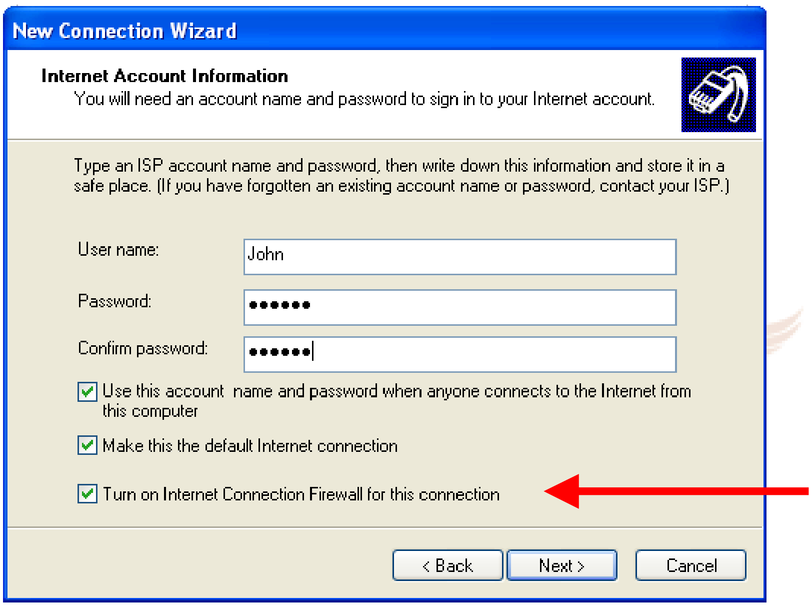
To continue, click Next.

Fig 5.3 New Connection Wizard

The New Connection Wizard is displayed to help the user through the process (figure 5.3). The main aim of the Wizard is to set up a new network connection. It appears that security, which is extremely important on a network, has been brushed over and ignored. The New Connection Wizard is taking an unobtrusive approach to security - perhaps too unobtrusive. Security does not seem to be a priority when it comes to creating network connections.

The ICF is not mentioned at this stage (figure 5.3). Security at this point is a support feature to the creation of a new network connection. It is not the main aim. However, at this stage the user should be informed that precautionary measures such as the ICF can be taken in order to improve the security of the new connection. This will help to alleviate any security fears which a user may have.

Only the steps of the Wizard which deal with the ICF are examined. The first step shown in figure 5.4 asks the user for their username and password.


New Connection Wizard

Internet Account Information

You will need an account name and password to sign in to your Internet account.

Type an ISP account name and password, then write down this information and store it in a safe place. (If you have forgotten an existing account name or password, contact your ISP.)

User name: John

Password: ••••••

Confirm password: ••••••

☑ Use this account name and password when anyone connects to the Internet from this computer

☑ Make this the default Internet connection

☑ Turn on Internet Connection Firewall for this connection

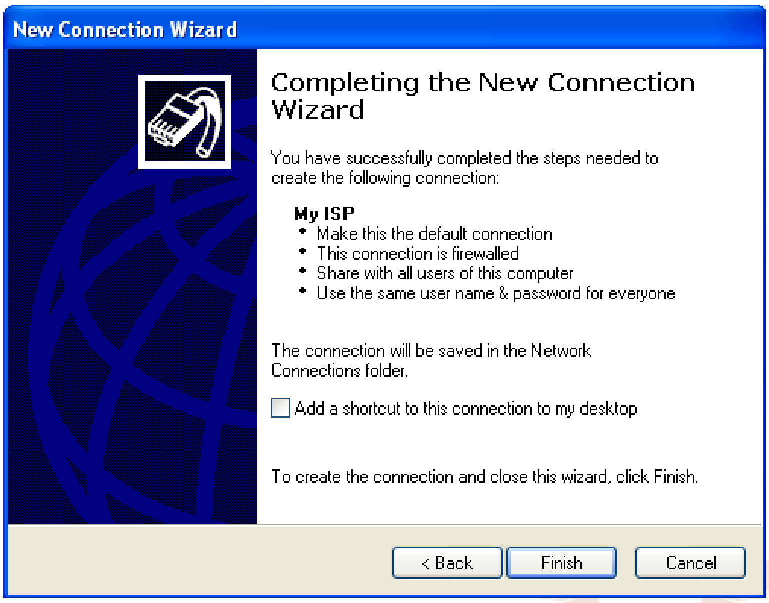
Fig 5.4 New Connection Wizard continued

Figure 5.4 is the only window which deals with the ICF. It is also the only window which informs the user about available security features. A user who is concerned about security (e.g. in the ABSA case) could be asking questions at this point such as "How safe is this connection?" and "What are my options to improve security?". The New Connection Wizard does not answer any of these questions.

Note that the Internet Connection Firewall is activated by default. This is a positive move as it simplifies the user's task. However, it may also lead to lack of *Trust* as there is no explanation of ICF at this stage. The *features* and importance of the ICF are not *conveyed* at this point.

This window has an *Aesthetic and minimalist design* and the user is not bombarded with information. By using a Wizard the information conveyed to the user is spread over a number of windows. However, there is no window which deals with security.

Once a user has completed all the steps in the New Connection Wizard the 'Completing the New Connection Wizard' (figure 5.5) is shown.



Completing the New Connection Wizard

You have successfully completed the steps needed to create the following connection:

My ISP
- Make this the default connection
- This connection is firewalled
- Share with all users of this computer
- Use the same user name & password for everyone

The connection will be saved in the Network Connections folder.

☐ Add a shortcut to this connection to my desktop

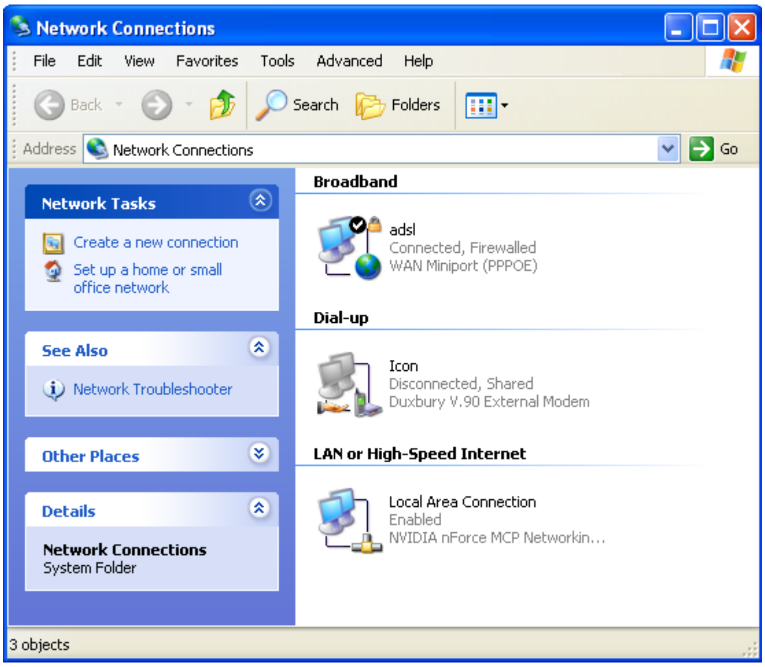
To create the connection and close this wizard, click Finish.

Fig 5.5 New Connection Wizard - complete

The creation of a new network connection and the activation of the ICF has almost been completed (figure 5.5).

The process has not been complicated or difficult. This is due to the fact that Windows XP has eliminated the normal firewall configuration hassles for consumers. There is, however, a major possibility that at this point the user is not aware that the ICF has been activated and may even be confused as to what a firewall is. Future versions of the ICF may incorporate outbound filtering. The ICF will then become even more important and useful as it will be able to provide a level of protection against spyware.

The settings for the ICF cannot be configured during the activation process. This can only be done after activation and then via the advanced settings (see the next section) of a connection. This limits the options available to the user during activation. The user wants to feel in control and that the process is flexible. Clicking on 'Finish' in figure 5.5 will take the user back to the 'Network Connections' window shown in figure 5.6.



Network Connections
System Folder

Broadband

adsl
Connected, Firewalled
WAN Miniport (PPPOE)

Dial-up

Icon
Disconnected, Shared
Duxbury V.90 External Modem

LAN or High-Speed Internet

Local Area Connection
Enabled
NVIDIA nForce MCP Networkin...

3 objects

Fig 5.6 Firewall is active

The new Internet connection is now activated (figure 5.6). Note the small padlock and 'Firewalled' text (shown by the red arrows), which means that the ICF will be active when this connection is used.

This padlock icon is only visible under Network Connections. It is quite easy for the user not to notice it, and therefore not to be aware that the ICF is active. The *Visibility of system status* is therefore not clear.

In this example a broadband ADSL connection was made. An added security risk of 'always-on' Internet connections such as ADSL and cable is that they are more susceptible to outside attacks. A dial-up connection, even though it may be vulnerable, is usually not connected to the Internet for long periods. ADSL is normally more frequently connected to the Internet, giving hackers more time to gain access to the user's computer. During the installation the user was not made aware that the ICF can provide a level of protection against this.

Table 5.2 shows the criteria which have been used to analyse the activation component of the ICF's interface. The blue 'Yes' does not mean that the criteria have been met, but rather that the criteria are relevant for the activation component. As can be seen from the table under *Errors,* an environment which generates errors could not be created.

Table 5.2 HCI-S criteria used in the analysis of the activation of ICF

Criteria	***Criteria used in analysis?***
Convey features	**Yes**
Visibility of system status	**Yes**
Learnability	**Yes**
Aesthetic and minimalist design	**Yes**
Errors	An environment which generated errors could not be created
Satisfaction	**Yes**

The configuration component of the interface is analysed in the next section.

5.5 Configuration of the ICF

The advanced features of the ICF can be configured by the user. There are a number of ways to access the settings for the ICF. As with the analysis of the activation of the ICF, it would be redundant to examine each one individually. One way is clicking 'Tools' and then 'Internet Options' in Internet Explorer. This is shown in figure 5.7.

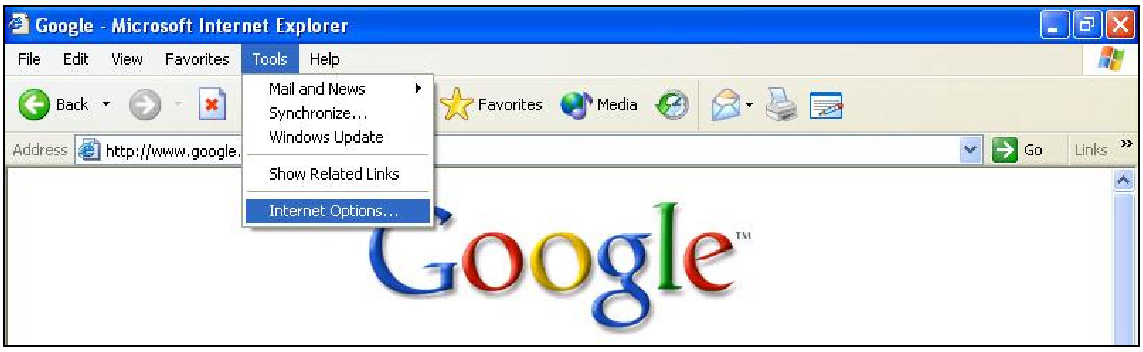
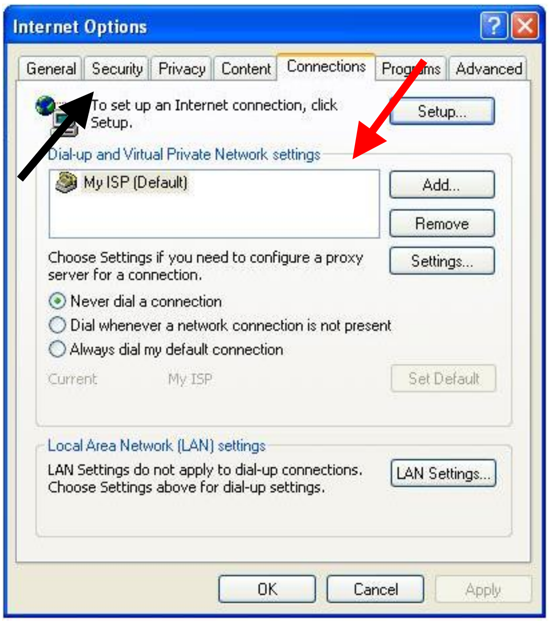


Fig 5.7 Internet Explorer

The 'Internet Options' window, figure 5.8, then opens. The black arrow points to the 'Security' tab. However, the configuration for the ICF is not found under this tab. The 'Security' tab deals with settings such as ActiveX permissions and file downloads. This means that a user who is trying to implement security features will not necessarily see the

ICF. Instead, the 'Connections' tab would need to be selected, followed by clicking the 'Settings' tab (figure 5.8).



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

To set up an Internet connection, click Setup. [Setup...]

Dial-up and Virtual Private Network settings

My ISP (Default)

[Add...] [Remove]

Choose Settings if you need to configure a proxy server for a connection. [Settings...]

● Never dial a connection
○ Dial whenever a network connection is not present
○ Always dial my default connection

Current: My ISP [Set Default]

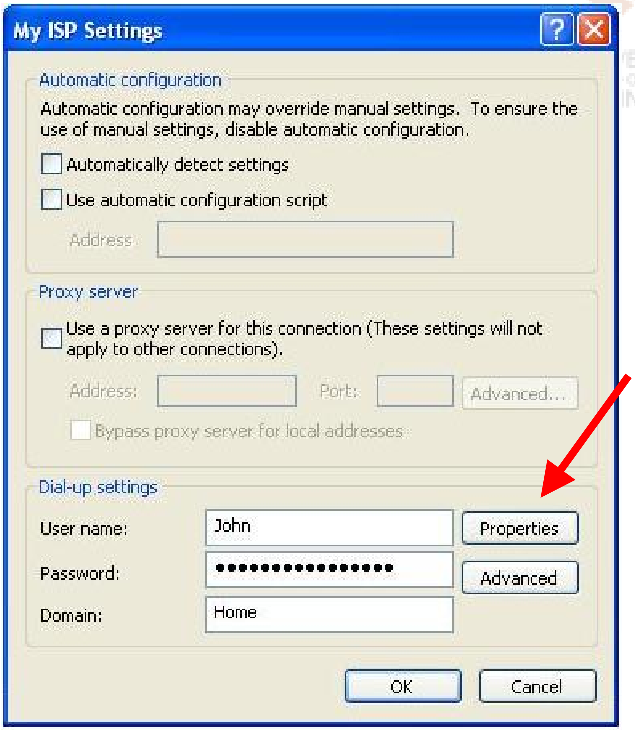
Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings. [LAN Settings...]

[OK] [Cancel] [Apply]

Fig 5.8 Internet Options

Clicking on the 'Settings' button generates the window shown in figure 5.9. The user now needs to click on the 'Properties' button in the 'My ISP Settings' window shown in figure 5.9. These steps are difficult for a user to *Learn.*



My ISP Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings
□ Use automatic configuration script

Address:

Proxy server

□ Use a proxy server for this connection (These settings will not apply to other connections).

Address: Port: [Advanced...]

□ Bypass proxy server for local addresses

Dial-up settings

User name: John [Properties]

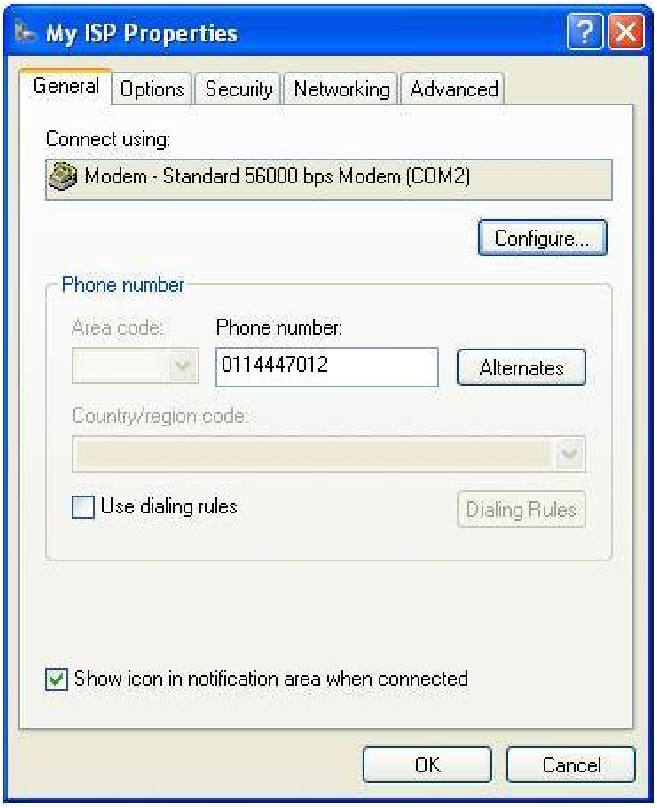
Password: •••••••••••••••• [Advanced]

Domain: Home

[OK] [Cancel]

Fig 5.9 My ISP Settings

Clicking on the 'Properties' button brings up the 'My ISP Properties' windows shown in figure 5.10.



Connect using:
Modem - Standard 56000 bps Modem (COM2)

Phone number:
0114447012

☐ Use dialing rules

☑ Show icon in notification area when connected

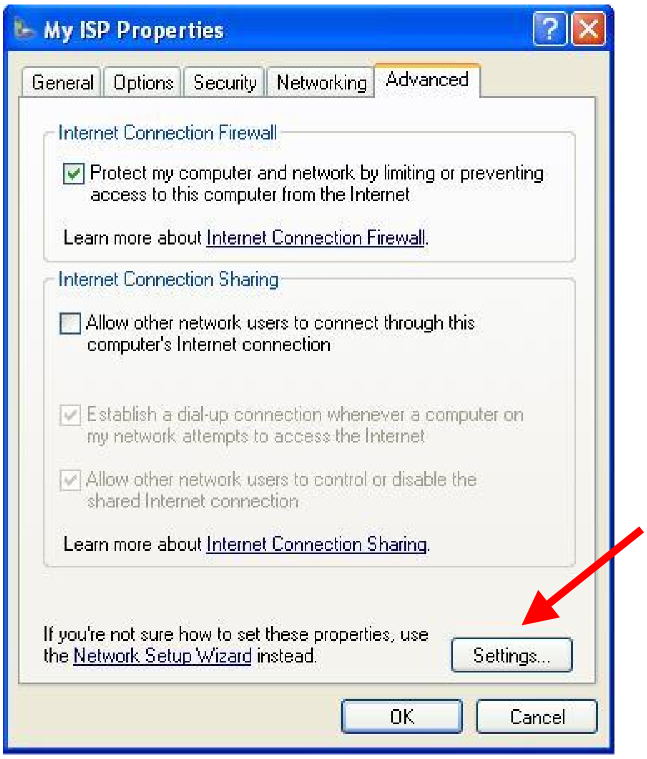
Fig 5.10 General settings

Once again, the 'Security' tab shown by the black arrow in figure 5.10 should not be selected. This tab leads to functions such as using an encrypted login.

Rather, the 'Advanced' tab needs to be selected (figure 5.10). This is not intuitive, as who decides which functions are advanced? It is also confusing that a 'firewall' would not be found under the heading of 'Security'.

This window (figure 5.10) is *Aesthetically* pleasing. There are a limited number of options available and the window has a clean layout.

Selecting the 'Advanced' tab presents the window shown in figure 5.11. In this window (figure 5.11) the user is able to activate or deactivate the ICF. This window has an *Aesthetic and minimalist design* (figure 5.11). It also has links to more information which should help the user to *Trust* the ICF. It is easier to trust something that is understood.



Internet Connection Firewall

☑ Protect my computer and network by limiting or preventing access to this computer from the Internet

Learn more about Internet Connection Firewall.

Internet Connection Sharing

□ Allow other network users to connect through this computer's Internet connection

☑ Establish a dial-up connection whenever a computer on my network attempts to access the Internet

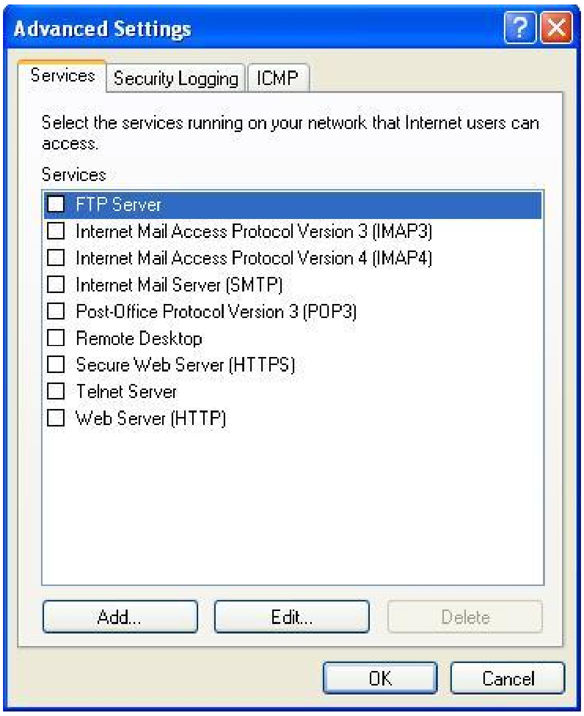
☑ Allow other network users to control or disable the shared Internet connection

Learn more about Internet Connection Sharing.

If you're not sure how to set these properties, use the Network Setup Wizard instead.

Fig 5.11 Advanced window

It is not obvious that the 'Settings' button at the bottom of the window, shown in figure 5.11, is also for the ICF. Clicking this button brings up a window with 'Advanced Settings', shown in figure 5.12.



Select the services running on your network that Internet users can access.

Services

□ FTP Server
□ Internet Mail Access Protocol Version 3 (IMAP3)
□ Internet Mail Access Protocol Version 4 (IMAP4)
□ Internet Mail Server (SMTP)
□ Post-Office Protocol Version 3 (POP3)
□ Remote Desktop
□ Secure Web Server (HTTPS)
□ Telnet Server
□ Web Server (HTTP)

Fig 5.12 Advanced settings

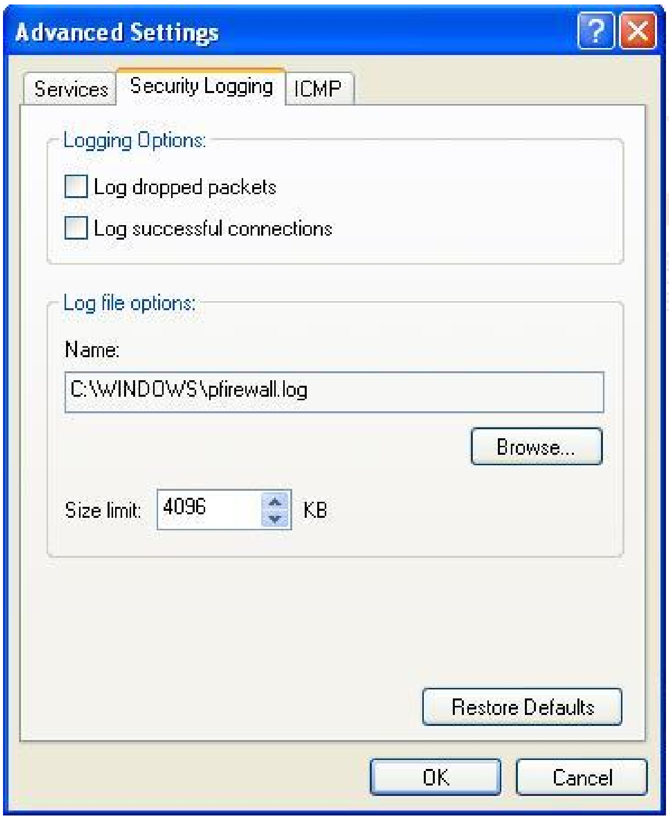
In the 'Advanced Settings' window, figure 5.12, there should be a label informing the user that these settings configure the ICF. At this point the user is also not warned about the danger of changing settings incorrectly.

The advanced settings for ICF are confusing and will probably never be used by the average user.

The 'Services' setting, figure 5.12, allows the user to run programs which would normally have been blocked by the firewall, for example a web server.

A description of each of these services is not given. Many users will not understand the purpose of this window.

Clicking on the 'Security Logging' tab in figure 5.12 brings up the window shown in figure 5.13.



Logging Options:

□ Log dropped packets

□ Log successful connections

Log file options:

Name: C:\WINDOWS\pfirewall.log

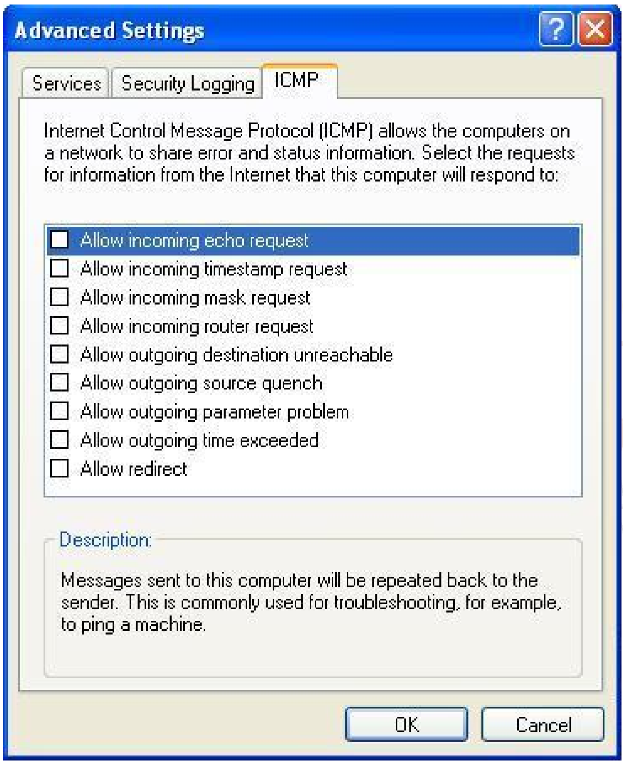
Size limit: 4096 KB

Fig 5.13 Security Logging

'Security Logging', shown in figure 5.13, allows the user to log the packets that the firewall has dropped. By default logging is off. The user then needs to manually open the log in a text file editor and look through it in order to see if there has been any suspicious activity. A size limit for the log file can be set to prevent the log file from filling up the user's hard drive. A summary function of the log file would have been useful. The *Visibility of system status* is therefore not clear.

The terminology used on this page (figure 5.13) is confusing, which hinders the *Learnability* of the system. For example, the term 'dropped packets' is a technical term, which many people might not understand.

Selecting the 'ICMP' tab shows the window in figure 5.14. 'ICMP' (Internet Control Message Protocol) sets the firewall to accept certain packets, for example a ping packet.



Internet Control Message Protocol (ICMP) allows the computers on a network to share error and status information. Select the requests for information from the Internet that this computer will respond to:

- □ Allow incoming echo request
- □ Allow incoming timestamp request
- □ Allow incoming mask request
- □ Allow incoming router request
- □ Allow outgoing destination unreachable
- □ Allow outgoing source quench
- □ Allow outgoing parameter problem
- □ Allow outgoing time exceeded
- □ Allow redirect

Description:

Messages sent to this computer will be repeated back to the sender. This is commonly used for troubleshooting, for example, to ping a machine.

Fig 5.14 ICMP

A description of each protocol is also given in figure 5.14. This aids the *Learnability* of the system. It also helps to develop *Trust* as a user is more likely to trust software which they understand.

It is not clear to the user that these advanced settings deal with the ICF.

Figure 5.14 is the last window concerned with the configuration of the ICF. Table 5.3 shows which criteria were used during the analysis of the configuration of the ICF. As with the activation component, all the criteria except for *Errors* have been used.

Table 5.3 HCI-S criteria used in the analysis of the configuration of ICF

Criteria	***Criteria used in analysis?***
Convey features	**Yes**
Visibility of system status	**Yes**
Learnability	**Yes**
Aesthetic and minimalist design	**Yes**
Errors	An environment which generated errors could not be created
Satisfaction	**Yes**

In the next section the operation of the ICF is analysed.

5.6 Operation of the ICF

The operation of the ICF is simple. Whenever a network connection is used, the ICF is active, provided the ICF option was selected when the network connection was created. For example, in the previous section a Wizard was used to create a new dial-up connection and the ICF option was checked. Whenever this dial-up connection is used, the ICF is active.

However, the user is not aware of this as there is no icon in the systems tray (figure 5.15). No message alerts the user to the fact that they are now protected. The *Visibility of system status* is therefore not at all clear.

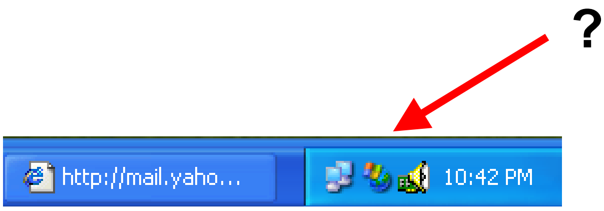


Fig 5.15 System tray

When a 'rogue' packet is identified by the ICF, it is dropped, but the user is not made aware of this. Dropped packets can be optionally logged in a text file. Once again, the *Visibility of system status* is poor. The user should be notified of a possible hacking attempt. The user can then decide if they want to ignore any further warnings. Checking the entries in a log file can be easily forgotten. The criterion of *Satisfaction* is therefore not handled well in this case. It could have been a very satisfying experience to know that an attempted hack had been thwarted!

If the future versions of the ICF implement outbound checking, then the importance of alerting the user to suspicious activity will increase. For example, when a program attempts to send data over a network connection for the first time, the user needs to be alerted immediately. This is because the program could be some form of spyware.

The operational component of the ICF interface is very limited. All the parts of the interface which deal with the operation of the ICF have therefore been examined. In the next chapter possible interfaces which allow the user to operate the ICF are demonstrated.

Table 5.4 shows the criteria which are used in the analysis of the operation of the ICF. As can be seen, five of the six criteria have been used.

Table 5.4 HCI-S criteria used in the analysis of the operation of ICF

Criteria	***Criteria used in analysis?***
Convey features	**Yes**
Visibility of system status	**Yes**
Learnability	**Yes**
Aesthetic and minimalist design	**Yes**
Errors	An environment which generated errors could not be created
Satisfaction	**Yes**

A summary of the analysis of the three components is presented in the next section.

5.7 Summary of analysis

The analysis has been broken down into the three components of activation, configuration and operation. For each component a total percentage is given representing the level of trust. On the one side of the scale there is absolute trust and on the other no trust at all. Between these two values there are many levels of trust. The percentage, based on how many HCI-S criteria were met, attempts to represent these different levels of trust. Trust can be very personal and is therefore difficult to quantify.

An explanation of the colours found in the summaries is given in table 5.5. If an HCI-S criterion is not met, then 0 is added to the overall score for a component (red). Green means the criterion has been met and 100% of the weighting is added to the score. Orange is between green and red. In this case 50% of the possible weighting for a criterion is added to the score.

Table 5.5 Key

Colour	***Explanation***	***Influence on weighting***
Red	Criterion has not been met.	0% of weighting
Green	Criterion has been met.	100% of weighting
Orange	In some instances the criterion has been met, in other instances it has not.	50% of weighting
Gray	Criterion is not applicable for this component.	

Each criterion is given a weighting for each component of the ICF. For example, in the activation component five criteria are used. This means that each criterion has a 20% weighting – 20% x 5 criteria = 100% total weighting.

The results of the activation component are presented in the next section.

5.7.1 Activation of ICF

During the activation process the ICF was compared against five of the six HCI-S criteria. The criterion of *Errors* has been left out. This is because during the testing of the ICF no error messages were generated. This does not mean, however, that it is error-free.

Table 5.6 Activation of ICF

Criteria	***Conclusion***	***Impact***	
Convey features (20% weighting)	**NO** The ICF is not explained.	The user is not aware of what the ICF is.	0%
Visibility of system status (20% weighting)	**NO** It is not clear from the interface whether the activation of the ICF was a success and that the new network connection is now protected by the ICF.	The user may not know that the ICF is active or if it is inactive.	0%
Learnability (20% weighting)	**YES** Activation is intuitive and easy.	When creating a new connection, the ICF will probably be activated by the user.	20%
Aesthetic and minimalist design (20% weighting)	**YES** The user is not bombarded with too many details. Technical information is kept to a minimum.	The user will not be swamped with information.	20%
Errors	An environment which generated errors could not be created.		
Satisfaction (20% weighting)	**Partial** Quick and easy to activate, which leads to *Satisfaction.* However, the user is not aware of what the ICF is or why it is important.	If the user is aware of the ICF, they may decide to ignore it or to purchase a different firewall.	10%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 50% level of trust has been developed.	**Total**	**50%**

The main reason why so few criteria are met during activation is that the user is not informed of the purpose of the ICF. It is also not clear to the user that the activation was a success (figure 5.6).

5.7.2 Configuration of ICF

The results of the analysis of the configuration component are presented in the following table:

Table 5.7 Configuration of ICF

Criteria	***Conclusion***	***Impact***	
Convey features (20% weighting)	**YES** More information is provided under the Advanced Settings window (figure 5.12). A description for each 'ICMP' is also given.	A user with some technical knowledge would be able to understand what features of the ICF can be configured.	20%
Visibility of system status (20% weighting)	**NO** It is not evident whether or not the ICF has been working correctly. A user would need to manually check a text file in order to see which packets have been dropped by the ICF.	The user will not be aware of what the ICF is doing. Unless the user manually checks the log file, they will not know if the firewall blocked any suspicious activity.	0%
Learnability (20% weighting)	**NO** The advanced features of the ICF are complex and would be difficult for a user to understand.	Most users will not be able to configure the ICF.	0%
Aesthetic and minimalist design (20% weighting)	**YES** The windows have a neat clean layout.	The user will find the windows pleasing to the eye.	20%

Criteria	*Conclusion*	*Impact*	
Errors	An environment which generated errors could not be created.		
Satisfaction (20% weighting)	**NO** The configuration of the ICF will not be a *Satisfying* experience for most users. The settings are difficult to find and the advanced functions are confusing.	Many users may not configure the ICF or examine the log file.	0%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 40% level of trust has been developed.	**Total**	**40%**

The configuration options of the ICF are difficult to find. It is also not obvious to a user that the advanced settings, e.g. 'Services' and 'ICMP' (figures 5.12 and 5.14), apply to the ICF. The activity of the ICF can be optionally logged in a text file. It is unlikely that a user will bother to open the text file and if they do, they probably will not understand it. These factors contribute to the ICF only meeting two of the possible six HCI-S criteria in table 5.7.

5.7.3 Operation of ICF

As was seen during the analysis of the ICF, the operation component scored poorly according to the HCI-S criteria. The results are shown in the following table:

Table 5.8 Operation of ICF

Criteria	*Conclusion*	*Impact*	*Score*
Convey features (20% weighting)	**NO** The ICF is not explained.	The user is not aware that a firewall is available.	0%

Criteria	*Conclusion*	*Impact*	*Score*
Visibility of system status (20% weighting)	**NO** It is not obvious if the ICF is active or working. The user is provided with little feedback.	It is easy for the user not to be aware of the ICF.	0%
Learnability (20% weighting)	**YES** Turning the ICF on and off is easy.	If the user knows that they have a firewall, they will probably be able to turn it on and off.	20%
Aesthetic and minimalist design (20% weighting)	**NO** The ICF does not have an interface while it is active!	It is very difficult to fine-tune the ICF during operation.	0%
Errors	An environment which generated errors could not be created.		
Satisfaction (20% weighting)	**NO** Most users will not even be aware that their computers can be protected by the ICF. If the ICF is active, the users will not know if it is dropping packets.	Users may consider purchasing a firewall which provides more feedback.	0%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 20% level of trust has been developed.	**Total**	**20%**

When it comes to operation (table 5.8) of the ICF, the interface is limited. The user is not made aware of the status of the ICF.

Overall the ICF scores poorly in establishing trust:

50%	during activation
40%	during configuration
20%	during operation

This gives the ICF an overall score of 37% (110 divided by 3 components). An overall score below 50% means that less than half of the criteria have been met. An interface which meets so few criteria is inadequate. If the overall score is between 50% and 60%, then the interface has scored below average. An overall score of 60%-70% is average. A score of 80%-90% means that the interface is above average and has met most of the criteria. A score above 90% is an excellent interface. The impact of the scores is shown in the following table.

Table 5.9 Description of scores

Overall score	***Description***	***Impact***
0%-49%	Inadequate interface	The user will avoid using the interface, which will lead to weak security.
50%-59%	Below average interface	The interface will confuse and frustrate the user.
60%-69%	Average interface	The user will tolerate the interface if they really need to use the program.
70%-85%	Above average interface	Most of the interface will be easy to use. One or two aspects of the interface may irritate the user.
86%-100%	Excellent interface	The user will enjoy using the interface. The implementation of security features by the user is easy and intuitive.

The interface of the ICF has therefore scored poorly. This means many users will not be aware of the ICF. If users are aware of it, they will find it difficult to configure and operate.

The HCI-S criteria are not infallible and their limitations are discussed in the next section.

5.8 Advantages and disadvantages of the six HCI-S criteria

The HCI-S criteria are not fool–proof and have some limitations. Based on this chapter's analysis, the following advantages and disadvantages have been identified.

One of the first advantages of the criteria is that there are only six criteria to remember. This means that when developing a new interface, a software engineer can keep the HCI-S criteria at the back of his or her mind. The criteria are also simple and easy to understand, which also leads to the easy recollection of the criteria.

Any interface can be analysed in a short time frame because there are only six criteria. The resulting analysis will give guidance as to the strengths and weaknesses of the interface from both an HCI and a security perspective.

Another advantage of the HCI-S criteria is that the criteria emphasise the importance of both usability and security. This helps a developer maintain the balance between security and usability.

When it comes to the limitations of the criteria, one disadvantage is that the criteria only provide a high level description of what is desired. Details are not provided. For example, the criterion of *Convey features* does not inform the developer exactly how to convey the security features. The developer needs to decide how to do this. Articles and design criteria are available which can assist a developer in this regard [USAB02]. These resources fall beyond the scope of this dissertation.

A second disadvantage is that the criterion of *Satisfaction* is difficult to quantify. One user may feel a sense of enjoyment when using a security feature, while another may be totally dissatisfied with exactly the same feature. This could be due to users' past experiences or personal preferences.

Another weakness is that the HCI-S criteria may be adequately met by the interface but the actual coding of the program could be weak, leading to a false sense of security. Applying the HCI-S criteria will not improve the technology behind the interface.

The HCI-S criterion of *Trust* is not solely dependent on the interface. The interface plays an important role in developing trust. However, factors such as the company's brick and mortar reputation also play a large role. Applying the HCI-S criteria cannot be viewed in isolation but need to be part of a larger company-wide strategy aimed at developing and growing customers' trust.

5.9 Conclusion

In this chapter the three components of activation, configuration and operation of the ICF were analysed according to the HCI-S criteria. This means that the first objective of this chapter has been met. Based on this analysis, a trust percentage figure for each component, and a total trust percentage for the entire interface was calculated. This figure has helped to identify the strengths and weaknesses of the interface so that in the following chapter recommendations can be made. These calculations have enabled the second objective to be met. During the analysis of the interface various advantages and disadvantages of the criteria were uncovered. These advantages and disadvantages have been highlighted and discussed, thus meeting the third objective. By meeting these objectives it has been shown that the HCI-S criteria can be used successfully in a real-world situation. The goal of the chapter has therefore been achieved.

The ICF is a powerful piece of software and a good addition to the Windows XP operating system. Even though the ICF did not obtain an adequate percentage according to the HCI-S criteria, it is an important step in ensuring that firewall software is used by all users. However, because of its poor interface, it is unlikely that the ICF is used by most users. As was highlighted in the ABSA case, the importance of security features is growing. Hopefully in the next version of Windows the interface of the ICF, especially the operation, will have been improved.

In the following chapter some recommendations are made on how the HCI-S of the ICF can be improved.

Chapter 6
Recommendations for Windows XP's Internet Connection Firewall

6.1 Introduction

In the previous chapter the interface of the Windows XP's Internet Connection Firewall was analysed. It is evident from chapter 5 that a number of the HCI-S criteria are not completely satisfied by the current interface of the ICF.

The aim of this chapter is to show how the ICF's interface can be changed to improve the security of a system by making it easier to use. In order to achieve this goal three objectives are set. The first objective is to improve the interface during the activation of the ICF, which should lead to a higher level of trust and better security. The second objective is to modify the interface so that the configuration of the ICF is easier. The third objective is to change the interface during the operation of the ICF so that it is more intuitive to use and that the user is made aware of the presence of the ICF.

There are different types of users who respond differently to interfaces. For this dissertation a distinction needs to be made between non-technical users and technical users. This distinction is necessary because the non-technical user does not have the same technical background as a technical user. There are certain security features in the firewall which should be used by all users and other features which a non-technical user cannot be expected to understand. By 'non-technical user' is meant a user who does not have in-depth computer knowledge. An example of a non-technical user is a business executive who is not involved in the IT sector and who uses computers for tasks such as email, word processing and Internet access. A technical user is someone who possesses comprehensive computer skills and is familiar with advanced computer concepts such as SSL, IP addresses, packets and secure servers.

In this chapter some recommendations are made for the interface of the ICF based on the criteria for a successful HCI-S (chapter 4). Following from these recommendations a new interface for the ICF is proposed. In chapter 5 the ICF was divided into three areas - activation of the ICF, configuration of the ICF and operation of the ICF. In this chapter recommendations are made in the same three areas (figure 6.1).

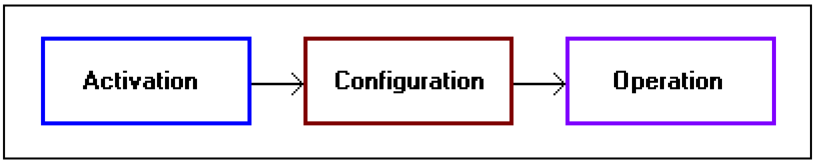
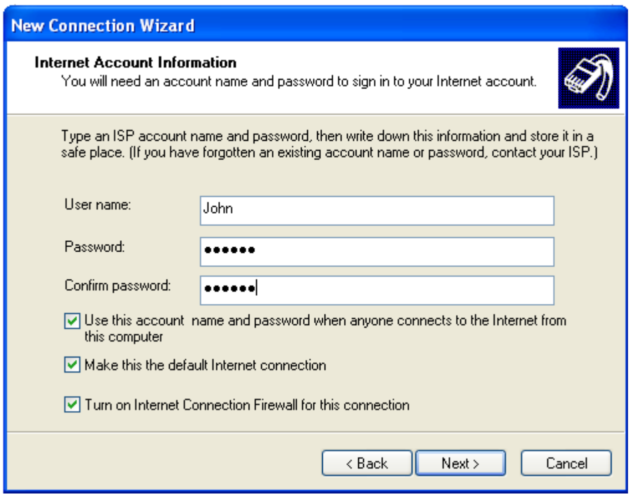


Fig 6.1 Chapter layout

Some of the screen grabs in this chapter are the same as the images in chapter 5. These duplicates have been included to make it easy to compare the existing interface with the proposed interface.

6.2 Activation

As was seen in chapter 5, the activation of the ICF is simple and easy. The user is given the option to turn the ICF on via a check box during the New Connection Wizard (figure 6.2). However, the ICF is not explained at this point, which leads to a lack of *Trust* as the user may not be aware of the function of a firewall. The *Learnability* of the system has also been hindered by the lack of an explanation of the firewall. It is difficult for the user to learn how to use the ICF when they do not even know what it is. The proposed changes are shown in figure 6.3.



New Connection Wizard

Internet Account Information

You will need an account name and password to sign in to your Internet account.

Type an ISP account name and password, then write down this information and store it in a safe place. (If you have forgotten an existing account name or password, contact your ISP.)

User name: John

Password: ••••••

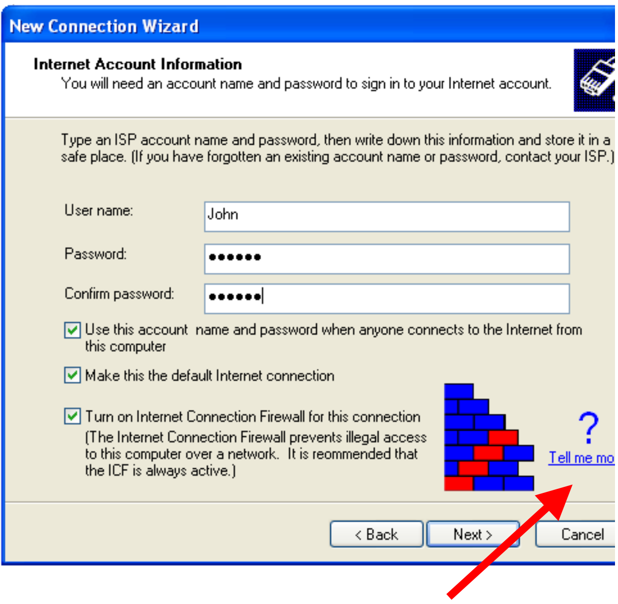
Confirm password: ••••••

☑ Use this account name and password when anyone connects to the Internet from this computer

☑ Make this the default Internet connection

☑ Turn on Internet Connection Firewall for this connection

Fig 6.2 Existing installation window of the ICF



New Connection Wizard

Internet Account Information

You will need an account name and password to sign in to your Internet account.

Type an ISP account name and password, then write down this information and store it in a safe place. (If you have forgotten an existing account name or password, contact your ISP.)

User name: John

Password: ••••••

Confirm password: ••••••

☑ Use this account name and password when anyone connects to the Internet from this computer

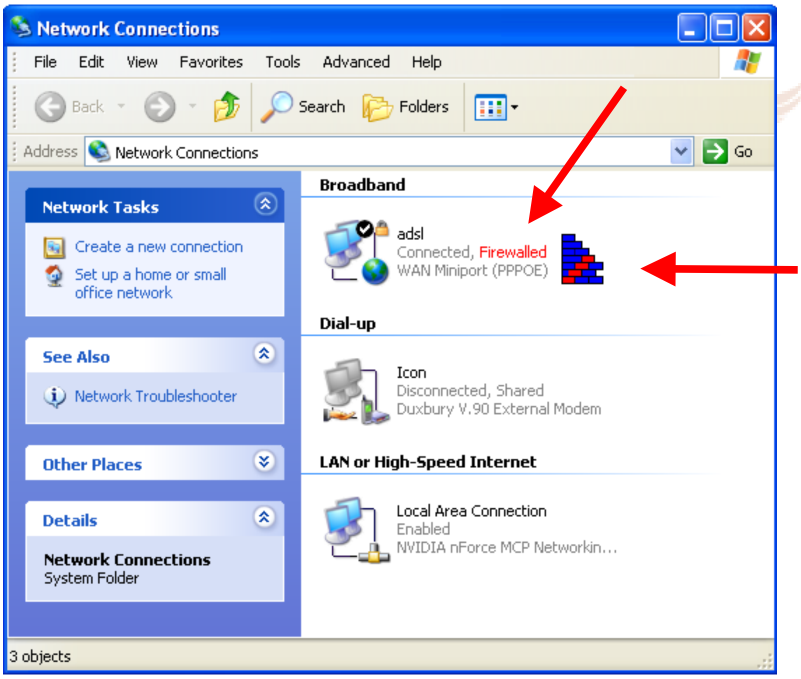
☑ Make this the default Internet connection

☑ Turn on Internet Connection Firewall for this connection
(The Internet Connection Firewall prevents illegal access to this computer over a network. It is reommended that the ICF is always active.)

Fig 6.3 Proposed installation window of the ICF [CORNE]

In order to satisfy the HCI-S criteria of *Trust* and *Learnability,* it is recommended that a brief explanation of the ICF be given at this stage (figure 6.3). An example of a possible explanation of the ICF is: "*The Internet Connection Firewall prevents illegal access to this computer over a network. It is recommended that the ICF is always active.*" This statement stresses the importance and function of the ICF. The user will now *Trust* the system more as the purpose of the ICF has been explained. A link should also be present that provides more detailed information. This detailed information will aid the *Learnability* of the system. A graphic of a wall has been introduced to improve the *aesthetics* of the window and to draw the user's attention to the firewall. This graphic is used later on to depict the presence of the ICF.

Once the ICF has been successfully activated, additional icons and text appear next to the connection in the existing Network Connections window (figure 6.4). These icons are small and, as was seen in chapter 5, the *Visibility of system status* is poor. In order to meet the criterion of *Visibility of system status,* an extra graphic and highlighted text (in red) have been added to the proposed interface (shown in figure 6.5). This draws the user's attention to the presence of the ICF on a network connection.



Network Connections
System Folder

Broadband

adsl
Connected, Firewalled
WAN Miniport (PPPOE)

Dial-up

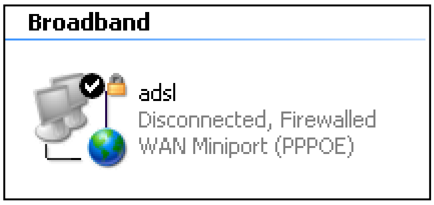
Icon
Disconnected, Shared
Duxbury V.90 External Modem

LAN or High-Speed Internet

Local Area Connection
Enabled
NVIDIA nForce MCP Networkin...

3 objects

Fig 6.5 Proposed Network Connections window


Broadband

adsl
Disconnected, Firewalled
WAN Miniport (PPPOE)

Fig 6.4 Existing Network Connections window

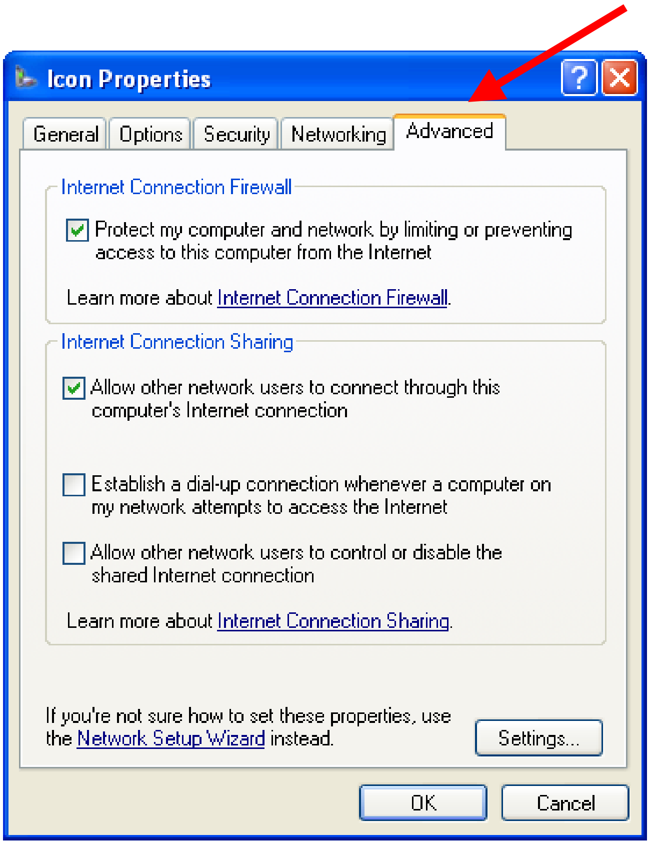
In the next section recommendations are made on how the interface can be improved during the configuration of the ICF.

6.3 Configuration

A number of changes can be made to the interface during configuration to improve the level of trust generated.

6.3.1 Icon properties

Once the ICF has been activated the user may need to configure it. Figure 6.6 shows the existing configuration window for the ICF. Figure 6.7 shows a screen shot of the proposed new configuration interface for the ICF.



Icon Properties

Internet Connection Firewall

☑ Protect my computer and network by limiting or preventing access to this computer from the Internet

Learn more about Internet Connection Firewall.

Internet Connection Sharing

☑ Allow other network users to connect through this computer's Internet connection

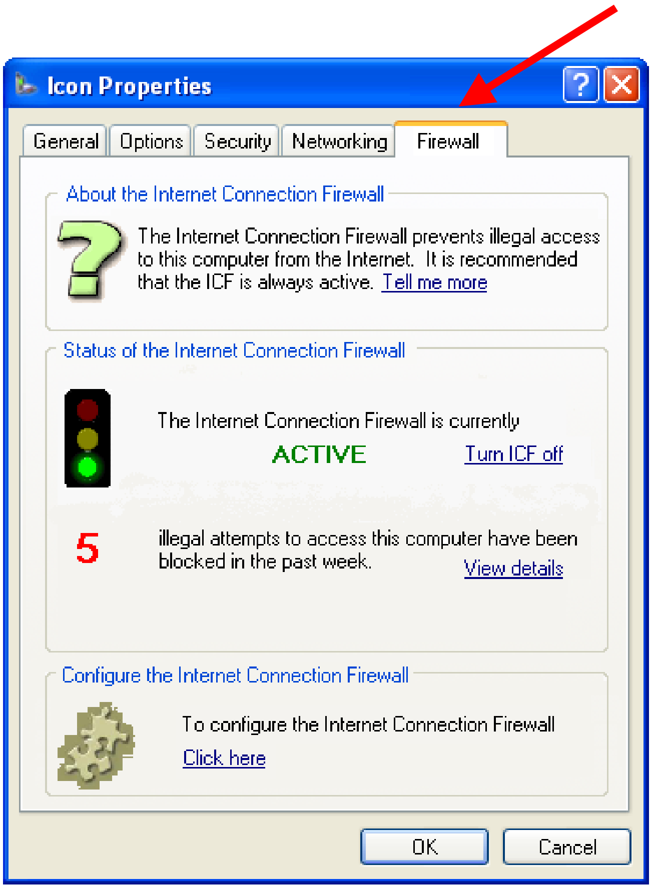
□ Establish a dial-up connection whenever a computer on my network attempts to access the Internet

□ Allow other network users to control or disable the shared Internet connection

Learn more about Internet Connection Sharing.

If you're not sure how to set these properties, use the Network Setup Wizard instead.

Fig 6.6 Existing HCI-S for the ICF



Icon Properties

About the Internet Connection Firewall

The Internet Connection Firewall prevents illegal access to this computer from the Internet. It is recommended that the ICF is always active. Tell me more

Status of the Internet Connection Firewall

The Internet Connection Firewall is currently

ACTIVE Turn ICF off

5 illegal attempts to access this computer have been blocked in the past week. View details

Configure the Internet Connection Firewall

To configure the Internet Connection Firewall Click here

Fig 6.7 Proposed interface for the Internet Connection Firewall [PUZZLE] [QUEST]

In the proposed interface (figure 6.7), the tab has been changed from 'Advanced' to 'Firewall'. Many technical users avoid any buttons or tabs with the word 'Advanced' on them. Some users feel that 'Advanced' settings should not be changed or explored as they only need to be used by technical users who are using their computer for out-of-the-ordinary tasks. The ICF, however, is not an advanced feature, but rather a standard feature that should be used by all users. The proposed interface (figure 6.7) focuses only on the ICF, unlike the existing interface which also deals with Internet Connection Sharing.

As was seen in chapter 5, the process to view the existing interface (figure 6.6) of the ICF is long and convoluted. In order to solve this problem there are three methods to view the proposed interface (figure 6.7) for the ICF:

1. Clicking on the 'F' in the system tray.
2. Selecting the ICF in the Windows Control Panel. This means that a new icon would need to be added to the Windows Control Panel for the ICF.
3. Clicking on the ICF tab when the user is reviewing any network connections, e.g. Internet connections or LAN connections.

These three methods are intuitive because they follow standard Windows XP user interface conventions. If a user is familiar with the Windows operating system then they should be able to open up the configuration window for the ICF. This aids the *Learnability* of the proposed interface.

The interface in figure 6.7 has an *Aesthetic and minimalist design.* This can be seen by the simple layout and it contains only relevant information for the ICF. The graphics make the window more interesting and less intimidating. The interface is as uncomplicated as possible and easy to *Learn.* This is because the window is based on recognition and not on recall. This means that the user does not need to remember how the ICF works but rather recognises what the functions do. The content of the window has been broken up into three parts – 'About the Internet Connection Firewall', 'Status of the Internet Connection Firewall' and 'Configure the Internet Connection Firewall'.

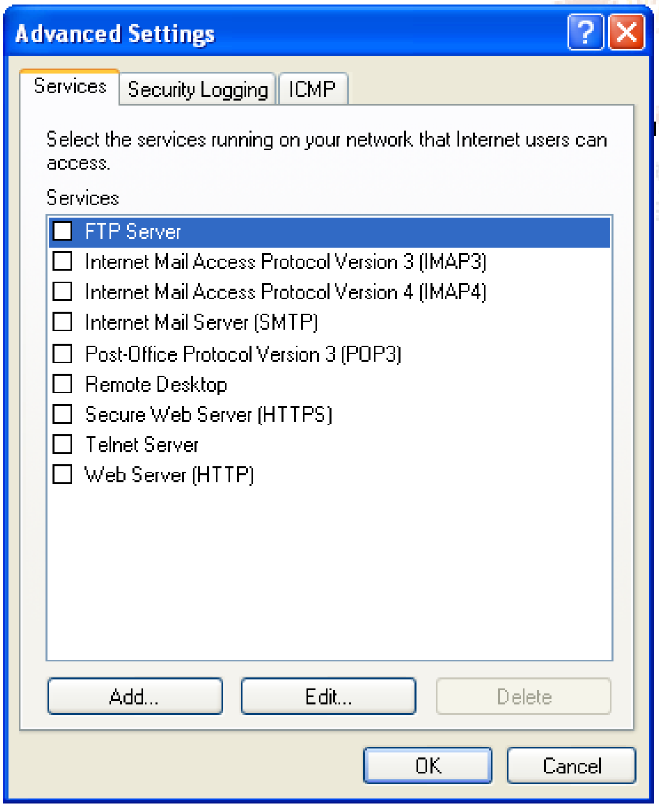
'About the Internet Connection Firewall' provides a brief explanation of the ICF along with a link to the Windows XP help file, which provides more information for the non-technical user. In addition to this, a web address is given in the help file which points the technical user to comprehensive, detailed and technical information on the ICF. The question mark graphic represents more information and draws the attention of the user to where more information can be found.

'Status of the Internet Connection Firewall' conveys the status of the firewall. The *Visibility of system status* is clearly displayed by the green 'Active' statement. The user is also informed of any possible hacking attempts. In this example '5' possible hacks have occurred. This encourages the user to *Trust* the ICF as they can see it working. A link, 'View details' is given which opens up the Log window (figure 6.11) which gives the exact details of the possible hacking attempts.

'Configure the Internet Connection Firewall' provides a link to the 'Settings' window (figure 6.9). The graphic of puzzle pieces helps to convey to the user that this section of the interface is concerned with the configuration of the ICF. Both technical and non-technical users can configure the ICF. Some configuration features, as discussed in the next section, would only be used by a technical user.

6.3.2 Advanced settings

In the existing ICF interface (figure 6.8) the advanced settings are divided into 'Services', 'Security Logging' and 'ICMP'. These settings are used to configure the ICF to work correctly under different circumstances. For example, the computer running the ICF may also be used as a web server. This means that certain packets, which would normally be blocked by a firewall, need to be allowed through. In the existing Advanced Settings interface (figure 6.8) it is not clear that these settings are for the ICF and will probably only ever be used by technical users.

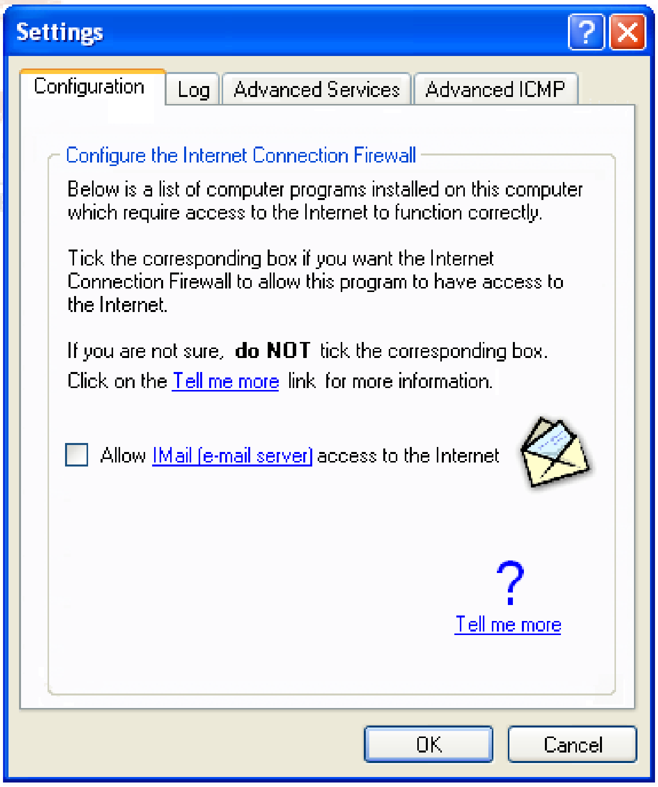


Select the services running on your network that Internet users can access.

Services

- □ FTP Server
- □ Internet Mail Access Protocol Version 3 (IMAP3)
- □ Internet Mail Access Protocol Version 4 (IMAP4)
- □ Internet Mail Server (SMTP)
- □ Post-Office Protocol Version 3 (POP3)
- □ Remote Desktop
- □ Secure Web Server (HTTPS)
- □ Telnet Server
- □ Web Server (HTTP)

Fig 6.8 Existing Advanced Settings window



Configure the Internet Connection Firewall

Below is a list of computer programs installed on this computer which require access to the Internet to function correctly.

Tick the corresponding box if you want the Internet Connection Firewall to allow this program to have access to the Internet.

If you are not sure, **do NOT** tick the corresponding box. Click on the Tell me more link for more information.

□ Allow IMail (e-mail server) access to the Internet

Fig 6.9 Proposed ICF interface – configuration [MAIL]

In the proposed ICF interface the Settings window has been divided into 'Configuration', 'Log', 'Advanced Services' and 'Advanced ICMP' (figure 6.9). This is similar to the existing ICF interface except that there is an extra tab 'Configuration' and the window has been renamed 'Settings' instead of 'Advanced Settings'. These changes have been made in order to convey to the user that some of the settings are not advanced and can be used by a non-technical user. This aids the *Learnability* of the interface as the non-technical user will explore these settings.

The four tabs of 'Configuration', 'Log' , 'Advanced Services' and 'Advanced ICMP' will now be looked at.

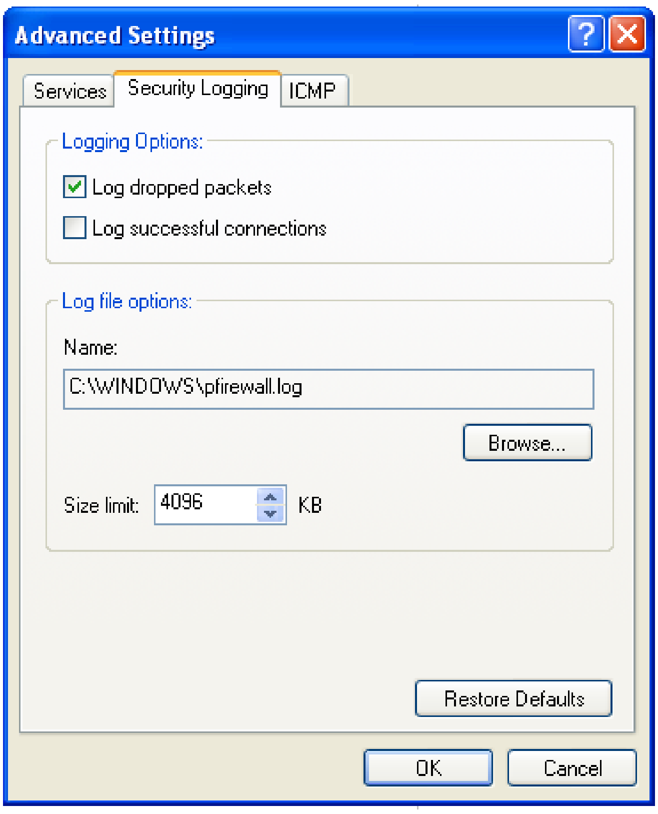
6.3.2.1 'Configuration' tab

The 'Configuration' tab, shown in figure 6.9, allows users who have a limited knowledge of computers to configure the firewall. This is done by listing all the programs which are installed on the user's computer whose network traffic may be blocked by the ICF. For example, figure 6.9 shows that an IMail email server has been installed on the computer. For this email server to work correctly, the ICF must allow certain packets which it would otherwise have blocked. The user is asked to tick the corresponding box if they want to allow a program to have access to the Internet. A 'Tell me more' link is provided which gives more detailed information.

Figure 6.9 also has an *Aesthetic and minimalist design.* Only relevant information is displayed and the user is not bombarded with too many options. This is achieved by only displaying programs which are currently installed whose functionality (sending and receiving over the network) may be blocked by the firewall. This will also draw the user's attention to any program which is installed of which they are not aware. By default all programs are blocked by the firewall (excluding Internet Explorer, Outlook and Outlook Express). The user is told not to allow access to a program if they are unsure.

6.3.2.2 'Log' tab

In the existing Log window (figure 6.10) the tab is called 'Security Logging'. In the proposed Log window (figure 6.11) the tab is now only called 'Log'. This is because in the proposed ICF interface it is obvious that the 'Log' relates to the Internet Connection Firewall.



Logging Options:

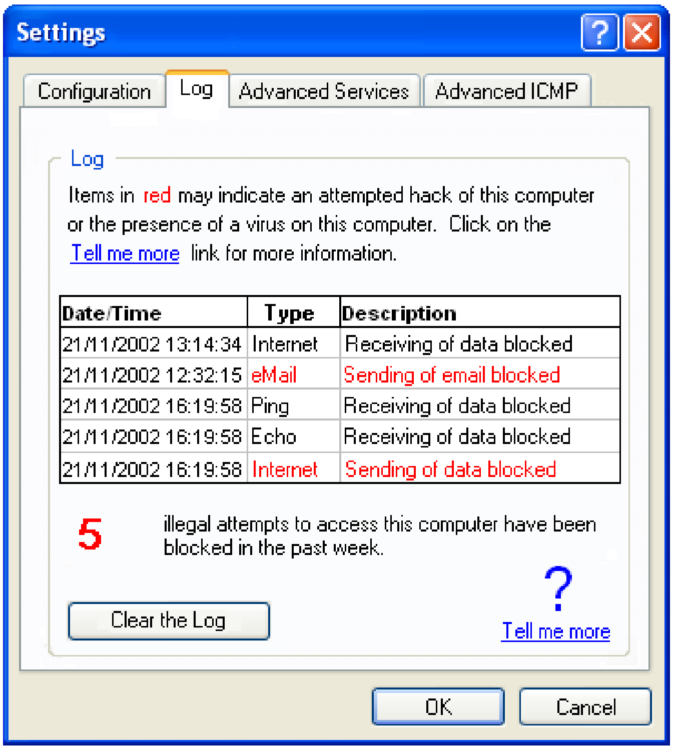
☑ Log dropped packets

☐ Log successful connections

Log file options:

Name: C:\WINDOWS\pfirewall.log

Size limit: 4096 KB



Log

Items in red may indicate an attempted hack of this computer or the presence of a virus on this computer. Click on the Tell me more link for more information.

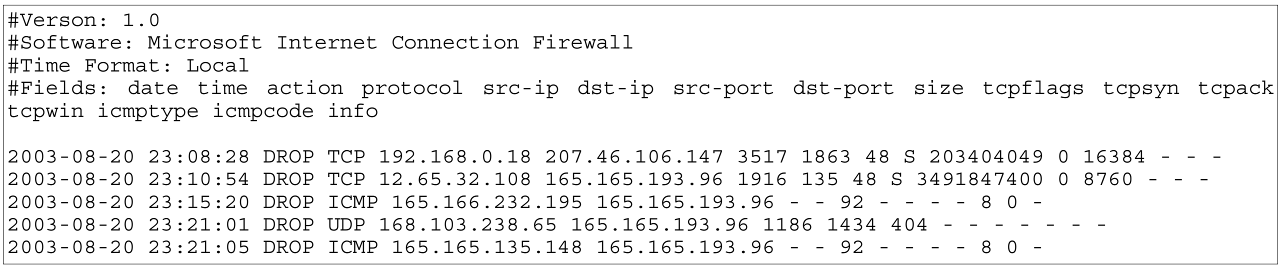
Date/Time	Type	Description
21/11/2002 13:14:34	Internet	Receiving of data blocked
21/11/2002 12:32:15	eMail	Sending of email blocked
21/11/2002 16:19:58	Ping	Receiving of data blocked
21/11/2002 16:19:58	Echo	Receiving of data blocked
21/11/2002 16:19:58	Internet	Sending of data blocked

5 illegal attempts to access this computer have been blocked in the past week.

Fig 6.10 Existing Log window

Fig 6.11 Proposed Log window

The existing ICF interface uses a text log file which is not easy to view (figure 6.12). The user has to manually find and open the text file in Windows Explorer. The content of the log file is also not easy to understand. As can be seen in figure 6.12 the log file is a 'jumble' of numbers and letters which very few users are able to understand.



```
#Verson: 1.0
#Software: Microsoft Internet Connection Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack
tcpwin icmptype icmpcode info

2003-08-20 23:08:28 DROP TCP 192.168.0.18 207.46.106.147 3517 1863 48 S 203404049 0 16384 - - -
2003-08-20 23:10:54 DROP TCP 12.65.32.108 165.165.193.96 1916 135 48 S 3491847400 0 8760 - - -
2003-08-20 23:15:20 DROP ICMP 165.166.232.195 165.165.193.96 - - 92 - - - - 8 0 -
2003-08-20 23:21:01 DROP UDP 168.103.238.65 165.165.193.96 1186 1434 404 - - - - - - -
2003-08-20 23:21:05 DROP ICMP 165.165.135.148 165.165.193.96 - - 92 - - - - 8 0 -
```

Fig 6.12 Existing log file

In the proposed interface (figure 6.11) the log file is interpreted for the user. The user is told of the date, time, type and description of the incident. For example, a packet was dropped on 21/11/2002 at 16:19:58. The type for this log item is 'Ping' and has a description of 'Receiving of data blocked'. This is easier for a user to understand compared to the existing log file. The type is there for the technical user so that they can quickly identify the nature of each log item.

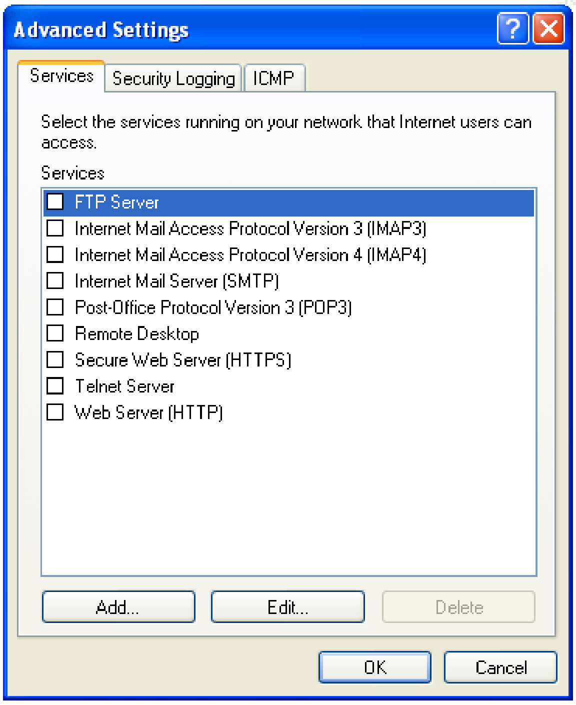
Log items which have the potential to be more serious, for example an email program trying to send an email which the user is not aware of, are highlighted in red. A 'ping' request is unlikely to be an attempted hack. It is therefore not in red.

These modifications add to the *Satisfaction* of using the ICF as a user can quickly and easily see any attempted intrusions. This log will also hopefully add to the *Trust* of the system as the user is able to see the ICF in action.

Visibility of system status is a crucial criterion in an HCI-S. The information in figure 6.11 will assist in fulfilling this criterion.

6.3.2.3 'Advanced Services' and 'Advanced ICMP' tabs

The proposed Advanced Services (figure 6.14) and proposed Advanced ICMP (figure 6.16) windows are similar to the existing ones (figures 6.13 and 6.15). This is because the usability of these windows is adequate for the technical user. These windows would only be accessed by a technical user who understands firewalls. The proposed ICF configuration window (figure 6.9) is a compromise, which allows the non-technical user to have access in a user-friendly manner to some of these advanced features.

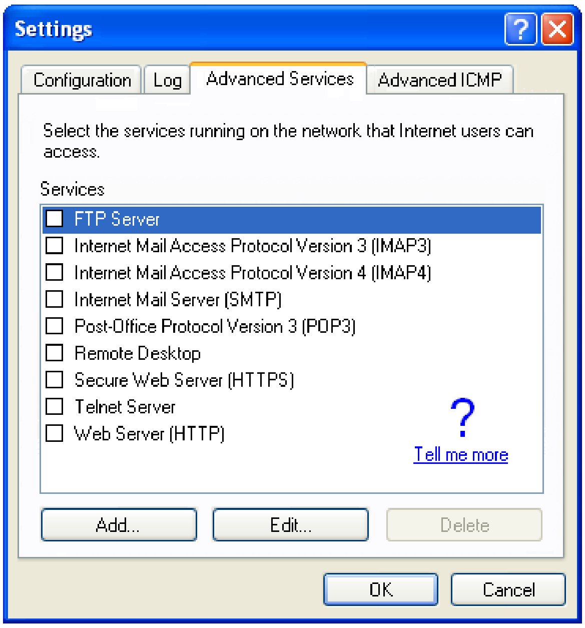


Advanced Settings

Select the services running on your network that Internet users can access.

Services

- □ FTP Server
- □ Internet Mail Access Protocol Version 3 (IMAP3)
- □ Internet Mail Access Protocol Version 4 (IMAP4)
- □ Internet Mail Server (SMTP)
- □ Post-Office Protocol Version 3 (POP3)
- □ Remote Desktop
- □ Secure Web Server (HTTPS)
- □ Telnet Server
- □ Web Server (HTTP)



Settings

Select the services running on the network that Internet users can access.

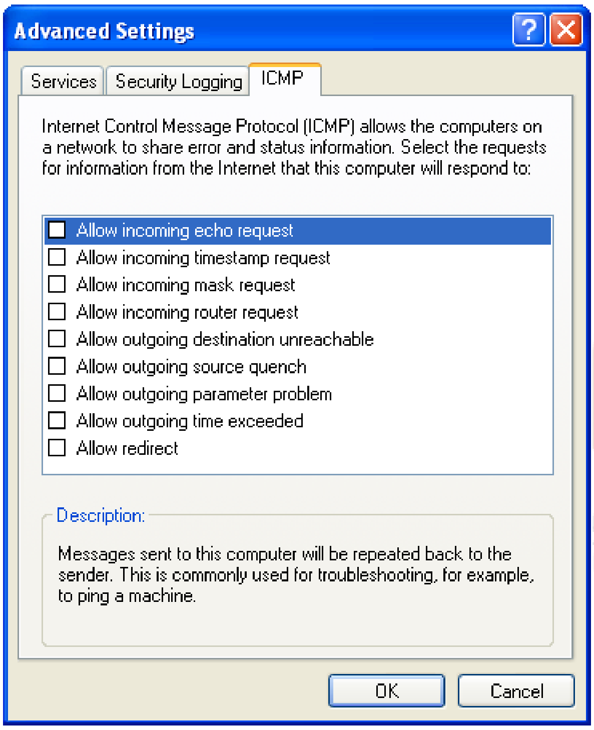
Services

- □ FTP Server
- □ Internet Mail Access Protocol Version 3 (IMAP3)
- □ Internet Mail Access Protocol Version 4 (IMAP4)
- □ Internet Mail Server (SMTP)
- □ Post-Office Protocol Version 3 (POP3)
- □ Remote Desktop
- □ Secure Web Server (HTTPS)
- □ Telnet Server
- □ Web Server (HTTP)

Fig 6.13 Existing Advanced Services Fig 6.14 Proposed Advanced Services

One difference between the proposed (figure 6.14) and existing Advanced Services window (figure 6.13) is the large question mark and 'Tell me more' link on the proposed interface. This link leads the user to the help file where more detailed information is given on what services are, and how to add, edit and delete them.

A similar question mark along with a 'Tell me more' link has also been placed prominently on the proposed Advanced ICMP window (figure 6.16). Detailed instructions on how to use the ICMP are also provided in the help file.

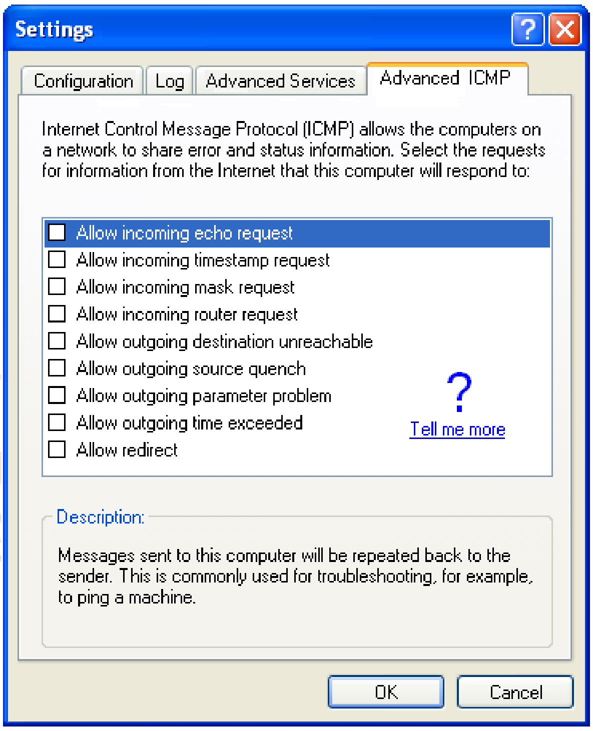


Internet Control Message Protocol (ICMP) allows the computers on a network to share error and status information. Select the requests for information from the Internet that this computer will respond to:

- ☐ Allow incoming echo request
- ☐ Allow incoming timestamp request
- ☐ Allow incoming mask request
- ☐ Allow incoming router request
- ☐ Allow outgoing destination unreachable
- ☐ Allow outgoing source quench
- ☐ Allow outgoing parameter problem
- ☐ Allow outgoing time exceeded
- ☐ Allow redirect

Description:

Messages sent to this computer will be repeated back to the sender. This is commonly used for troubleshooting, for example, to ping a machine.



Internet Control Message Protocol (ICMP) allows the computers on a network to share error and status information. Select the requests for information from the Internet that this computer will respond to:

- ☐ Allow incoming echo request
- ☐ Allow incoming timestamp request
- ☐ Allow incoming mask request
- ☐ Allow incoming router request
- ☐ Allow outgoing destination unreachable
- ☐ Allow outgoing source quench
- ☐ Allow outgoing parameter problem
- ☐ Allow outgoing time exceeded
- ☐ Allow redirect

Description:

Messages sent to this computer will be repeated back to the sender. This is commonly used for troubleshooting, for example, to ping a machine.

Fig 6.15 Existing ICMP window

Fig 6.16 Proposed Advanced ICMP window

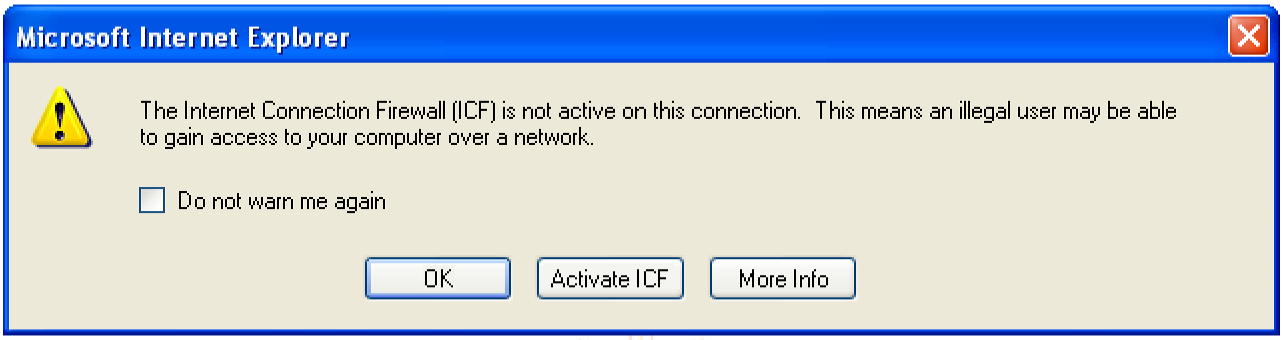
In the next section, recommendations are made in the crucial area of the operation of the ICF.

6.4 Operation

As was seen in chapter 5, the existing interface of the ICF does not clearly inform the user of the status of the ICF. The interface during the operation of the ICF is non-existent. The user does not know if the ICF is active or what the ICF is doing. This means that the user is unlikely to *Trust* something of which they are not aware. The lack of an interface during operation also hinders the *Visibility of system status*, and limits the *Satisfaction* a user gets from using the ICF.

A number of recommendations follow in the next paragraphs which aim to improve the operation of the ICF.

In the proposed interface a message box is displayed as soon as a network connection is used that is not protected by the ICF, warning the user. The user then has the option to ignore the warning or activate the ICF. Clicking on the 'More Info' button brings up additional details on what the ICF is and why it is important to activate it. The message box aids the *Visibility of system status* as the user is informed of the status of the ICF on a network connection. Figure 6.17 shows a proposed message box.



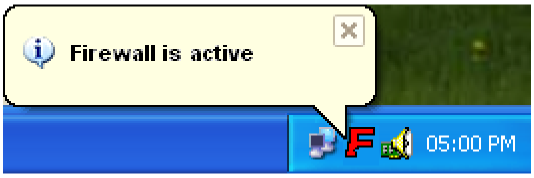
Microsoft Internet Explorer

The Internet Connection Firewall (ICF) is not active on this connection. This means an illegal user may be able to gain access to your computer over a network.

☐ Do not warn me again

Fig 6.17 Proposed message box - ICF not active

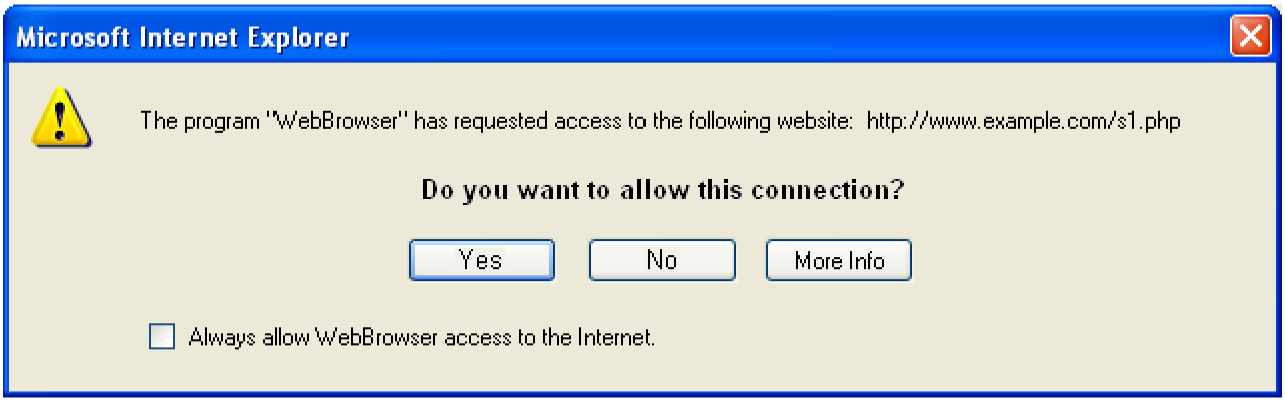
In the proposed interface an icon is also added to the system tray whenever the ICF is active, in this case an 'F' for firewall (figure 6.18). Clicking on the 'F' brings up the firewall window (figure 6.7). Windows users are already familiar with the system tray and should be comfortable with the operation of these icons. This aids the *Learnability* of the proposed interface. A user also expects any running programs to be in the system tray on the task bar.



Firewall is active

Fig 6.18 Proposed icon in the system tray

If a program that has not been configured by the user (figure 6.9) attempts to send data over a network connection, then the ICF warns the user via a proposed message box (figure 6.19). The user can turn this option on and off.



Microsoft Internet Explorer

The program "WebBrowser" has requested access to the following website: http://www.example.com/s1.php

Do you want to allow this connection?

□ Always allow WebBrowser access to the Internet.

Fig 6.19 Proposed message box – notifies the user of requested connections

In the next section the proposed interface's trust weighting will be determined and compared to the existing interface's trust weighting.

6.5 Comparison between existing and proposed HCI-S

In the previous chapter the existing interface for the ICF was analysed according the HCI-S criteria and a 'trust weighting' was calculated. In this section the proposed interface is subjected to the same weighting mechanism. The goal is to see if the proposed interface has a higher level of trust than the existing interface. A higher score indicates an interface which is more likely to be successfully used by a user. The scores are calculated for the interface in the areas of activation, configuration and operation. A final combined score will then be calculated.

Text in red indicates a criterion that has not been met, green indicates that the criterion has been met and orange shows that in some cases the criterion has been met and in others it has not. (Refer to table 5.5 in chapter 5 for more detail.)

6.5.1 Activation of ICF – proposed interface

Table 6.1 below refers to the activation of the ICF. At the end of the table both the existing and the proposed interface scores are given.

Table 6.1 Activation of ICF

Criteria	***Existing interface***	***Proposed interface***	***New score***
Convey features (20% weighting)	**NO** The ICF is not explained.	**YES** The 'Tell me more' links inform the user of the security features.	20%
Visibility of system status (20% weighting)	**NO** It is not clear from the interface whether the activation of the ICF was a success and that the new network connection is now protected by the ICF.	**YES** Extra graphics, which are easy to see, have been added to show when a connection is protected by the ICF.	20%
Learnability (20% weighting)	**YES** Activation is intuitive and easy.	**YES** Ease of use is maintained.	20%
Aesthetic and minimalist design (20% weighting)	**YES** The user is not bombarded with too many details. Technical information is kept to a minimum.	**YES** The simple design during activation has been retained.	20%
Errors	An environment which generated errors could not be created.	Proposed interface should not generate any new errors.	
Satisfaction (20% weighting)	**Partial** Quick and easy to activate, which leads to *Satisfaction.* However, the user is not aware of what the ICF is or why it is important.	**YES** The ICF is explained in detail and the successful activation of the ICF is easily noted by the user.	20%
Does the interface lead to trust being developed?			

Criteria	*Existing interface*	*Proposed interface*	*New score*
Trust (100% weighting)	A 50% level of trust has been developed.	A 100% level of trust has been developed.	

During activation the proposed interface attains a 100% level of trust according to the HCI-S criteria. This is an improvement over the 50% level of trust scored by the existing interface. The main reason for this improvement is that in the proposed interface the user is informed of the purpose of the ICF, while in the existing interface the ICF is not explained. This is a small change which makes a huge impact on the level of trust.

The score of 100% means that the user will find the implementation of security features easy and intuitive. A score of 100% does not mean that the interface is perfect. It means that it has adequately met the HCI-S criteria. However, it can still be improved. The important consideration with the weighting is whether it has increased or decreased.

6.5.2 Configuration of ICF – proposed interface

Table 6.2 below shows the improvement of the proposed interface over the existing interface during configuration.

Table 6.2 Configuration of the ICF

Criteria	*Existing interface*	*Proposed interface*	*New score*
Convey features (20% weighting)	**YES** More information is provided in the help file for the Advanced Settings window (figure 6.13). A description for each 'ICMP' is also given.	**YES** Existing help is maintained and additional information given.	20%

Criteria	*Existing interface*	*Proposed interface*	*New score*
Visibility of system status (20% weighting)	**NO** It is not evident whether or not the ICF has been working correctly. A user would need to manually check a text file in order to see which packets have been dropped by the ICF.	**YES** Text file has been interpreted for the user (figure 6.11) and a summary given (figure 6.7) of the firewall's activities.	20%
Learnability (20% weighting)	**NO** The advanced features of the ICF are complex and would be difficult for a user to understand.	**Partial** Figure 6.9 is a compromise which gives the non-technical user access to some advanced features. However, some features (figures 6.14 & 6.16) are still complex and difficult for the non-technical user to understand.	10%
Aesthetic and minimalist design (20% weighting)	**YES** The windows have a neat clean layout.	**YES** Clean layout has been kept; additional windows have the same look and feel.	20%
Errors	An environment which generated errors could not be created.	Proposed interface should not generate any new errors.	

Criteria	*Existing interface*	*Proposed interface*	*New score*
Satisfaction **(20% weighting)**	**NO** The configuration of the ICF will not be a *Satisfying* experience for most users. The settings are difficult to find and the advanced functions are confusing.	**Partial** The satisfaction of using the interface has been improved as the user is better able to see what the ICF has been doing (figure 6.11). However, some features are still difficult to use.	10%
Does the interface lead to trust being developed?			
Trust **(100% weighting)**	A 40% level of trust has been developed.	An 80% level of trust has been developed.	

During the configuration of the ICF the proposed interface scores an 80% level of trust. This is a huge improvement over the existing interface. This score indicates that most of the security features will be easy to use, but there are still some aspects (e.g. the advanced features) which may be difficult and confusing to use.

The *Learnability* of the proposed ICF interface is not completely met due to the complicated advanced settings needed for a firewall to work correctly. In the proposed ICF interface a compromise has been suggested by having a separate configuration window (figure 6.9) which allows the non-technical user to set up some of the features of the ICF. However, the advanced services (figure 6.14) and advanced ICMP (figure 6.16) are still needed.

6.5.3 Operation of ICF – proposed interface

During the operation of the ICF the interface is non-existent. This means that the proposed interface is a huge improvement. This is shown in table 6.3 below.

Table 6.3 Operation of the ICF

Criteria	***Existing interface***	***Proposed interface***	***New score***
Convey features (20% weighting)	**NO** The ICF is not explained.	**YES** More information is available by clicking on the 'F' in the system tray.	20%
Visibility of system status (20% weighting)	**NO** It is not obvious if the ICF is active or working. The user is provided with little feedback.	**YES** Visibility of system status is clear through the use of an icon in the system tray (figure 6.18) and via message boxes (figures 6.17 & 6.19).	20%
Learnability (20% weighting)	**YES** Turning the ICF on and OFF is easy.	**YES** The use of icons in the system tray is familiar to most users. This aids the *Learnability* of the ICF.	20%
Aesthetic and minimalist design (20% weighting)	**NO** The ICF does not have an interface while it is active!	**YES** The user is only made aware of the ICF when necessary.	20%
Errors	An environment which generated errors could not be created.	Proposed interface should not generate any new errors.	

Criteria	***Existing interface***	***Proposed interface***	***New score***
Satisfaction **(20% weighting)**	**NO** Most users will not even be aware that their computers can be protected by the ICF. If the ICF is active, the users will not know if it is dropping packets.	**YES** The inclusion of the icon in the system tray should improve the user's experience.	20%
Does the interface lead to trust being developed?			
Trust **(100% weighting)**	A 20% level of trust has been developed.	A 100% level of trust has been developed.	

The proposed interface during operation obtains a score of 100%. The main reason for the major improvement in score is that the HCI-S criteria of *Convey features* and *Visibility of system status* have now been met. This leads to the criterion of *Satisfaction* also being met.

Now that activation, configuration and operation have been looked at in detail, a summary is given in the next section.

6.5.4 Trust weightings summarised

Overall the proposed interface has a trust weighting of 93% (table 6.4). This is a vast improvement over the existing interface. A higher trust weighting indicates that the interface is more intuitive, easier to use and understand, and will foster a higher degree of trust in the user. The greater the degree of trust a user has in a security feature, the more likely they are to implement it.

Table 6.4 Summary

	Existing interface	***Proposed interface***
Activation	50%	100%

	Existing interface	***Proposed interface***
Configuration	40%	80%
Operation	20%	100%
Average	**37%**	**93%**

The HCI-S criteria have been successfully used to analyse and make recommendations for the interface of the ICF. The increase in the trust weighting is proof that the HCI-S criteria can be used to improve a security interface. The HCI-S criteria can be used to improve not only the ICF, but also any security interface. Most of the changes to the interface suggested are cosmetic and do not require any changes to the functionality of the firewall.

6.6 Conclusion

In this chapter a proposed interface for the ICF has been presented. The first objective of this chapter was to improve the interface during activation. The trust weighting during activation has increased, thus illustrating that the first objective has been met. The second objective, making the configuration easier, has been achieved by the introduction of the proposed interface. This is reflected in the higher trust weighting that the proposed interface has achieved over the existing interface. The third objective, which was to make the operation of the interface more intuitive and to make the user aware of the ICF, has been achieved by the introduction of an icon in the system tray and the development of various message boxes.

By meeting the objectives, it has been shown that the interface can be improved by applying the HCI-S criteria. This means that users who would probably never have used the ICF before now hopefully will. An interface which is easy to understand and use will lead to the correct operation of the available security features. This leads to the user's computer being more secure, thus achieving the aim of the chapter, which was to improve the security of a system by improving the interface.

The hard work of coding the firewall has already been done, which means that only a few simple modifications (demonstrated in the proposed ICF interface) need to be made which will greatly enhance the user’s experience.

The concept of how HCI-S criteria relate to interfaces found on the Internet is explored in the next chapter.

Chapter 7
HCI-S and E-commerce

7.1 Introduction

"The Internet follows a kind of Sheer Design Darwinism: survival of the easiest" Jakob Nielsen [DONA00]

A web presence offers a business the opportunity to reach users worldwide at any time and almost anywhere. Regardless of the goal and mission of a website, without an effective layout, design and functionality, visitors will not return. Firstly, a website needs to be found by a potential customer and then it needs to keep the customer by being usable and easy to navigate. Then the website needs to provide a reason for the user to buy the product or service [WEBP].

With traditional computer software the user first purchases the application and then experiences its usability. However, on the Web, usability comes first as the user starts out by experiencing the usability of a site. Only if the site is easy to use will the user continue browsing.

Websites do not usually come with a training lesson or a manual. The user needs to be able to quickly understand the functioning of a website after scanning the home page. If a user becomes frustrated with a website, a competitor is just a click away. A positive experience with a website will hopefully lead to a loyal user and repeat purchases [NIEL00].

The size of the web population has increased dramatically. The Web is no longer only used by technologically minded people. This means that web designers must assume that their websites will be used by users who have a limited knowledge of technology. The goal for web designers is to produce websites which are easy to use, fast and intuitive for all users [SULL01].

Websites on the Internet can be broadly categorised into sites which accept or facilitate payments from users, for example e-commerce or banking websites, and websites which do not accept payments online, for example news and information sites. The focus of this dissertation is on HCI and security and the following chapters therefore concentrate on websites where security is essential, such as e-commerce and banking sites.

One of the main concerns of users who utilise e-commerce and banking websites is security. Users are hesitant to use e-commerce solutions because they do not have complete trust in the website or do not understand the technology that ensures that the transactions are secure. It is therefore important for the interface to foster trust in the user, preferably with an easy-to-understand logon procedure. HCI-S on the Web attempts to strike a balance between the seemingly opposing goals of usability and security. Usability attempts to make the website as easy to use as possible, and to convey in a non-complicated manner the security features available. Security, on the other hand, tries to make it as difficult as possible for an unauthorised user to compromise the security of the site. For example, from a security point of view, a user should have two randomly generated passwords which contain numbers and characters. Two randomly generated passwords are less susceptible to a brute force attack than a password which a user has chosen. However, from a usability standpoint, the shorter the passwords and the fewer passwords, the better [NIEL01].

The aim of this chapter is to develop the HCI-S criteria further so that they may be used to analyse security interfaces found in an e-commerce environment. In order to achieve this goal, a number of objectives need to be met. The first objective of this chapter is to see whether HCI principles play an important role in a web-based environment. Once this has been achieved, the second objective is to determine if the HCI-S criteria need to be adapted so that they can be used in a web environment. This is necessary because the HCI-S criteria are used in later chapters to analyse various interfaces found on the Internet. The third objective is to determine which functional components of a website relate to security and which HCI-S criteria apply to each functional component.

The first part of this chapter gives an overview of HCI by looking at why usability is important on the Internet. Following this, the criteria for a successful HCI-S are adapted to suit the Web. Next, various websites are looked at to see which components make up the HCI-S of a website. These components are then described and the relationship between them and the HCI-S criteria established.

7.2 The importance of HCI on the Web

In a study performed by Forrester Research consisting of 8 900 Internet users, it was found that there were four main reasons why a user would return to a website: high quality content, frequent updates, minimal download time and ease of use. HCI is directly concerned with the last reason, ease of use. Many websites, however, are difficult to use. The result is poor user satisfaction, and with e-commerce sites, disappointing sales.

Incorporating HCI principles in planning, design and evaluation will lead to a more user-friendly website [OPTA02].

HCI principles such as intuitive and efficient navigation, ease of use in finding a product or service, adequate feedback as to the status of a transaction and clear indications of the options available are important on the Internet. The benefit of applying HCI principles is a site which is user-friendly, lets users feel in control and allows appropriate flexibility, while providing interaction that appears simple [OPTA02].

In the brick and mortar world a customer's opinion of a company or business is based on many factors such as the location of the business, the décor, friendliness and service from the staff, and the range of stock. This means that for a business to be competitive in the physical world it needs to have an attractive appearance, which can be costly. However, on the Internet, when it comes to appearance, the playing field is level. To develop an attractive and user-friendly site is not prohibitively expensive compared to a mediocre one. The user may sometimes only be exposed to a company through its website, such as Amazon.com, which means the user does not have a physical location on which to base their opinion of a company. Factors such as trust, professionalism, value and class can be fostered through the website. A professionally designed site which is easy to use can have a huge impact on customer satisfaction. However, on the Web it is also very easy for a user to switch to a competitor's site. This places even more importance on the interface of the website [SKIDM].

Over the past five to eight years there has been a change from purely informational websites to sites which offer more interaction. Some websites have become a showcase for the latest technology. However, technology should not be the driving force in the development of a website, but rather it should be used to meet the users' needs, for example to allow a user to purchase an item online. This is where HCI can be used to implement technology solutions that meet users' needs on the Internet [OPTA02].

Research by User Interface Engineering (www.uie.com) shows that people cannot find the information they are looking for on websites about 60% of the time. According to Forrester Research, a poorly designed site can lead to [GOV1]:

- Losing approximately 50% of the potential sales from a site as people cannot find what they need.

- Losing repeat visits from 40% of the users who do not return to a site when their first visit resulted in a negative experience.

The above figures show that HCI principles have been neglected in the design of websites. A website may be creative and have an attractive appearance, but it should still be easy to understand and use.

The number of users on the Web has been growing dramatically each year, which means that there are always new users. On average 1 out of every 15 users on the Internet has been browsing for less than a month [SULL02]. This means that many users are still learning how the Web works and it cannot be assumed that the users have a basic knowledge of security features.

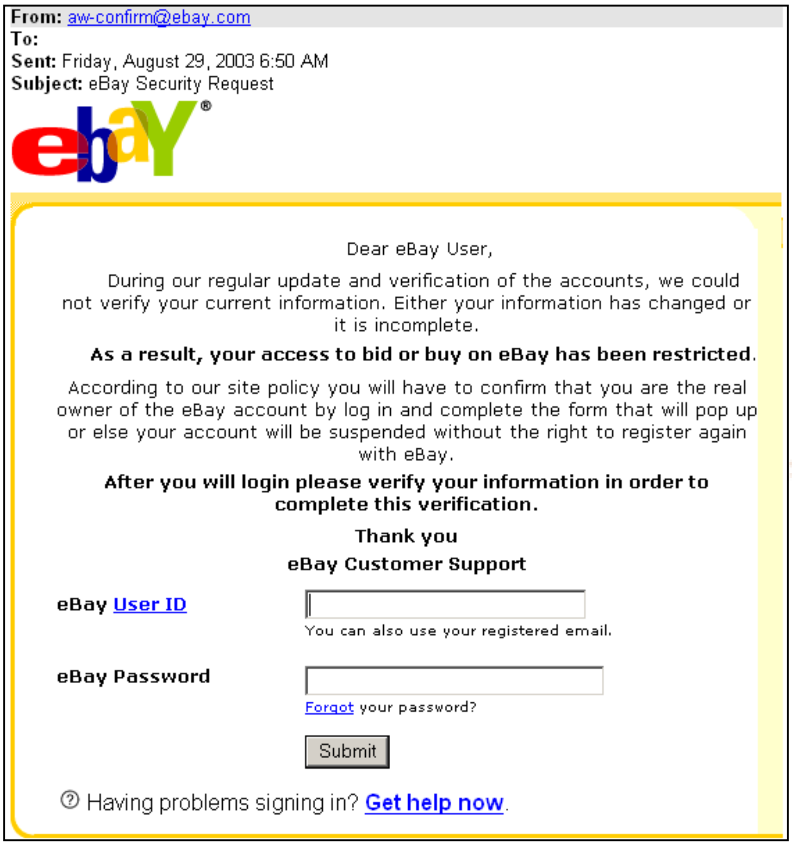
The above paragraphs have highlighted the importance of usability when in comes to web interfaces. The purpose of this is to provide the reader with background knowledge to interfaces found on the Internet. The focus of this dissertation, however, is on the security aspect of HCI. In the next section HCI-S criteria for the Web are discussed.

7.3 The importance of HCI-S on the Web

In the previous section (7.2) it was seen that HCI plays an important role with regard to interfaces on the Internet. This dissertation, however, focuses on the security aspects of interfaces. It is now necessary to determine whether HCI-S is important when relating to web interfaces.

The Internet has been evolving at a rapid pace. The Internet first started off providing static web pages and basic email. Here the main use and advantage of the Internet was the easy access to information. Now the Internet has progressed to instant messaging, e-commerce and online banking. As the Internet evolves, security has become more and more important. Initially the first users of the Internet were technically minded; now many users of the Internet have very little knowledge of computers and security. This means that the interface is extremely important in that this is how the user interacts with a web page. If the interface does not encourage and promote good security practices, then it is unlikely that the user will. The HCI needs to evolve as the Internet evolves.

One of the most troubling scams on the Internet, according to the FBI, is phishing. This is where a fraudulent email is sent to thousands of users. The email looks like it has come from an official company and normally asks the user to enter their username and password on the email or to visit a certain website. Figure 7.1 shows an example of an email that appears to have come from eBay. The interface presented in the email looks authentic as it has the correct logos and colours. If a user follows the link and fills in their details, their details will be compromised. In some cases the fraudulent email or web page even asks for credit card numbers and pin codes.



From: aw-confirm@ebay.com
To:
Sent: Friday, August 29, 2003 6:50 AM
Subject: eBay Security Request

Dear eBay User,

During our regular update and verification of the accounts, we could not verify your current information. Either your information has changed or it is incomplete.

As a result, your access to bid or buy on eBay has been restricted.

According to our site policy you will have to confirm that you are the real owner of the eBay account by log in and complete the form that will pop up or else your account will be suspended without the right to register again with eBay.

After you will login please verify your information in order to complete this verification.

Thank you
eBay Customer Support

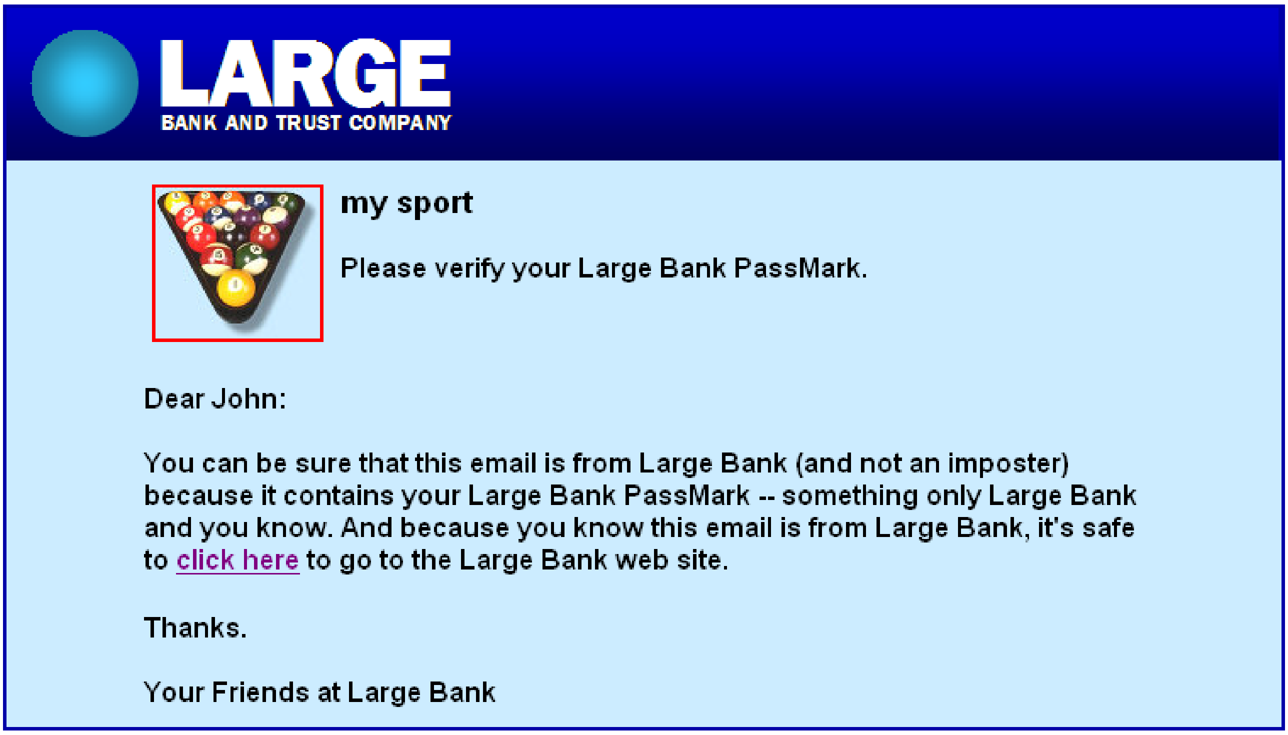
eBay User ID
You can also use your registered email.

eBay Password
Forgot your password?

Having problems signing in? **Get help now**.

Fig 7.1 eBay phishing [PRIVA03]

Phishing is not an easy threat to solve. Adding extra security to the server will not counter this scam. Instead, a possible solution can be found by adding some extra components to an interface. One company doing this is PassMark Security. During registration, each user selects their own unique picture. The customer is then encouraged to only deal with a company through a website or email if their unique picture is displayed. Figure 7.2 shows an example of a PassMark email which shows the user's unique graphic [PASS04].



LARGE
BANK AND TRUST COMPANY

my sport

Please verify your Large Bank PassMark.

Dear John:

You can be sure that this email is from Large Bank (and not an imposter) because it contains your Large Bank PassMark -- something only Large Bank and you know. And because you know this email is from Large Bank, it's safe to click here to go to the Large Bank web site.

Thanks.

Your Friends at Large Bank

Fig 7.2 Example of a PassMark [EMAIL04]

PassMark is an example which highlights the growing importance of interfaces on the Internet and how a security threat can be countered by changes in the interface.

Another example which illustrates the importance of interfaces in a security environment on the Internet is the use of keypads to counter spyware and key logging software. Some banks (www.absa.co.za, www.standardbank.co.za) have added an on-screen keypad for entering PINs (figure 7.3). Standard Bank has also chosen to randomise the keypad. The use of a keypad, both in random and traditional order, increases the security of the website. However, from a usability point of view it takes longer to enter the PIN using the on-screen keypad and it is more difficult to use.

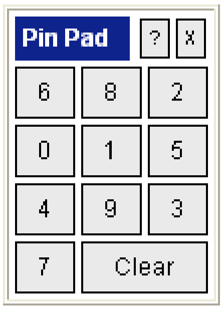


Fig 7.3 Keypad for Internet banking log on [STAND]

From the above examples it can be seen that HCI-S is definitely important in a web environment. In the next section the criteria for a web HCI-S are discussed.

7.4 Criteria for a web HCI-S

In comparing a web interface and a standard software interface, the underlying criteria (see chapter 4) for HCI are similar. However, there are some additional points for some of the criteria that need to be considered when dealing with web interfaces. The principles behind interfaces found in the traditional software environment and those found on the Internet are similar, but there are some differences which are highlighted in table 7.1. These differences lead to the criteria being modified.

Table 7.1 Differences between traditional software applications and web applications

	Traditional Software Application	***Web Application***
Status of user	User is known to a certain extent	User is unknown
Level of training	User may have received training	User has not received training
Type of user	Internal user	External user
Origin of software	Proprietary or developed in house	Usually custom developed
Intrinsic level of trust	Relatively high	Relatively low

Traditional software is often purchased from a reputable supplier, comes with a user manual and support numbers to call if needed. A website, on the other hand, does not necessarily have all of these default advantages. This means that the level of trust in a traditional software product, even before it has been used, is normally higher than it is for web applications.

The updated criteria are discussed below. New criteria have not been added, but the existing criteria have been modified.

7.4.1 Convey features

The security features available on a website need to be conveyed clearly to a user in a manner which is easy to understand. Some of the security features which the interface of a website needs to convey in an easily understandable manner are:

- The presence of SSL and encryption
- How usernames and passwords work
- The use of digital certificates
- Whether the security of the website has been verified by a third party (e.g. eTrust)

This is important because many users are not aware of the technology which can be used to provide a secure browsing experience. It is not necessary for the user to understand exactly how the technology works, but it is important for them to be informed what measures have been taken to ensure security and why this is important.

Figure 7.4 shows an example of a portion of an Internet banking home page. Two security features – SSL and certificates – are conveyed to the user by the use of the 'padlock' icon (bottom right) and the VeriSign Secure Site icon.

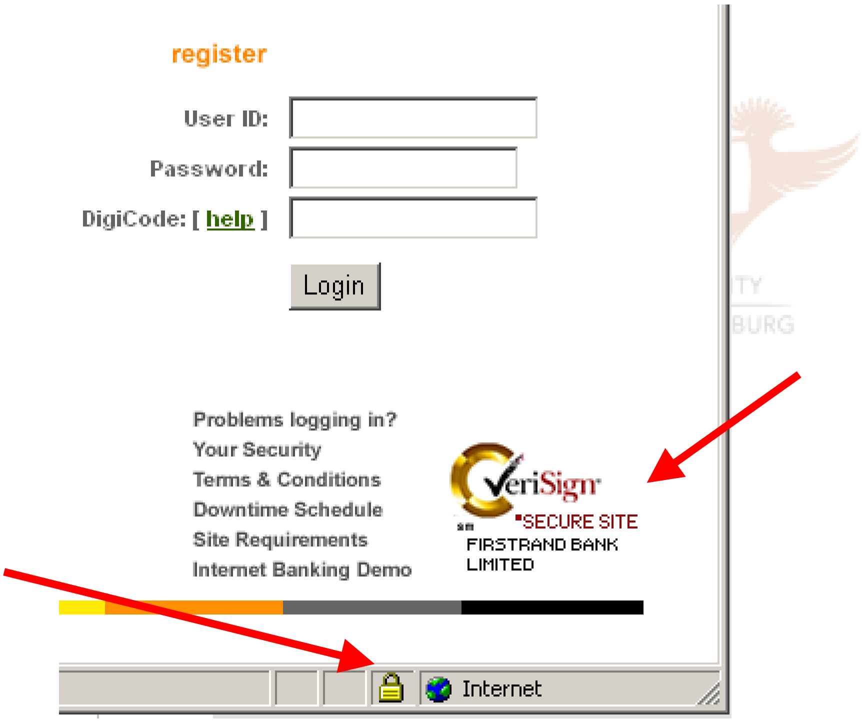
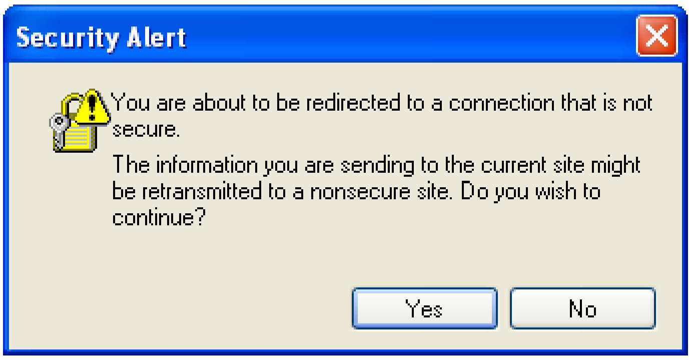


Fig 7.4 Conveying security features [EBUCKS]

7.4.2 Visibility of system status

The status of the security features must be evident to the user. For example, a message box may be necessary to assure the user that their credit card details are encrypted.

The criterion of *Visibility of system status* also needs to ensure that the user's attention is drawn to the security status of a connection. Figure 7.5 gives an example of a message box which warns the user that they are being redirected to a connection which is not secure. This helps the user to be aware of the system status.



Security Alert

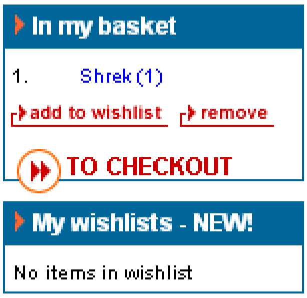
You are about to be redirected to a connection that is not secure.

The information you are sending to the current site might be retransmitted to a nonsecure site. Do you wish to continue?

Fig 7.5 Redirection warning

7.4.3 Learnability

Popular websites (e.g. Amazon.com and Yahoo.com) have set standards on how a user expects a web interface to work. This means that in some cases doing something different from the norm is not ideal. For example, most users expect to find a shopping cart at an e-commerce site. It would be ill-advised to therefore develop an e-commerce site which does not have a shopping cart. Even if users only buy one item, they still expect to be able to put it in their 'shopping cart' or 'basket' and proceed to the 'checkout'. Figures 7.6 and 7.7 show examples of shopping baskets which should be familiar to most users who have shopped online. Even though the shopping baskets are from two different companies, they are very similar.

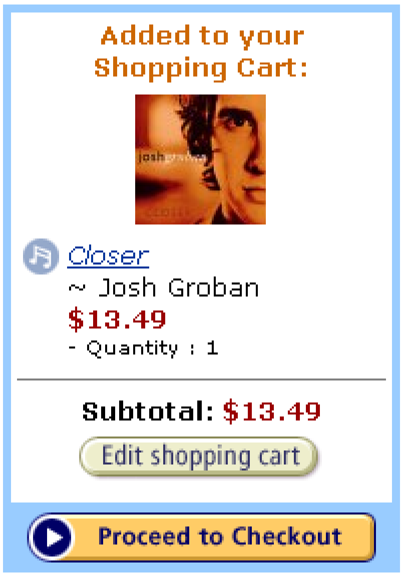


In my basket

1. Shrek (1)

My wishlists - NEW!

No items in wishlist



Added to your Shopping Cart:

Closer

~ Josh Groban

$13.49

- Quantity : 1

Subtotal: $13.49

Fig 7.6 Shopping basket (Kalahari.net) *Fig 7.7 Shopping basket (Amazon.com)*

An interface which is easy to learn is also an interface which behaves in a predictable way. The user must be able to predict what will happen when an action is taken. Predictability on the Internet is difficult because of the lack of strong design standards. For example, in the Windows environment most menus, pointers and icons are consistent and act in a predictable manner when clicked [DHER00]. However, each website has the potential to behave in a totally different manner. The importance of predictability*,* apart from ease of use and *Learnability*, is that it assists the development of *Trust* between the user and a website. The reasoning for this is discussed in paragraph 7.5 “HCI-S criteria lead to trust”.

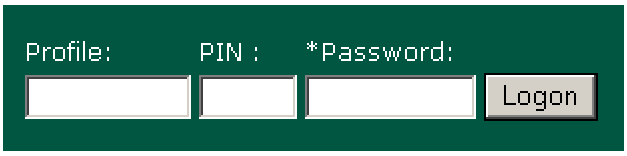


Figure 7.8 shows an example of the logon details required for a banking website. In this example the interface does not behave in a predictable manner. This is because the term 'Profile' is confusing. Is the website expecting a bank account number? Or perhaps a special username? It would have been less confusing if a term had been used with which online users are familiar, such as username, email address, or account number.

Fig 7.8 Banking website logon [NET]

Another way that the *Learnability* of a website can be improved is by allowing a certain level of flexibility. This means that there is more than one way for a user to accomplish a task. This helps the user to feel in control of the system.

7.4.4 Aesthetic and minimalist design

Speed on the Web is extremely important. Users do not want to wait for a page to download. Current recommendations are for a website to take 10 seconds or less to download [NIEL00]. Some possible ways that this can be achieved are to:

- Avoid large graphics and sound files.

- Use stylesheets and tables instead of graphics.
- Have more pages with less content on each page.
- Have a skip intro link as shown in figure 7.9.
- Display small pictures of products, and allow the user to click on the image to see a higher resolution picture.

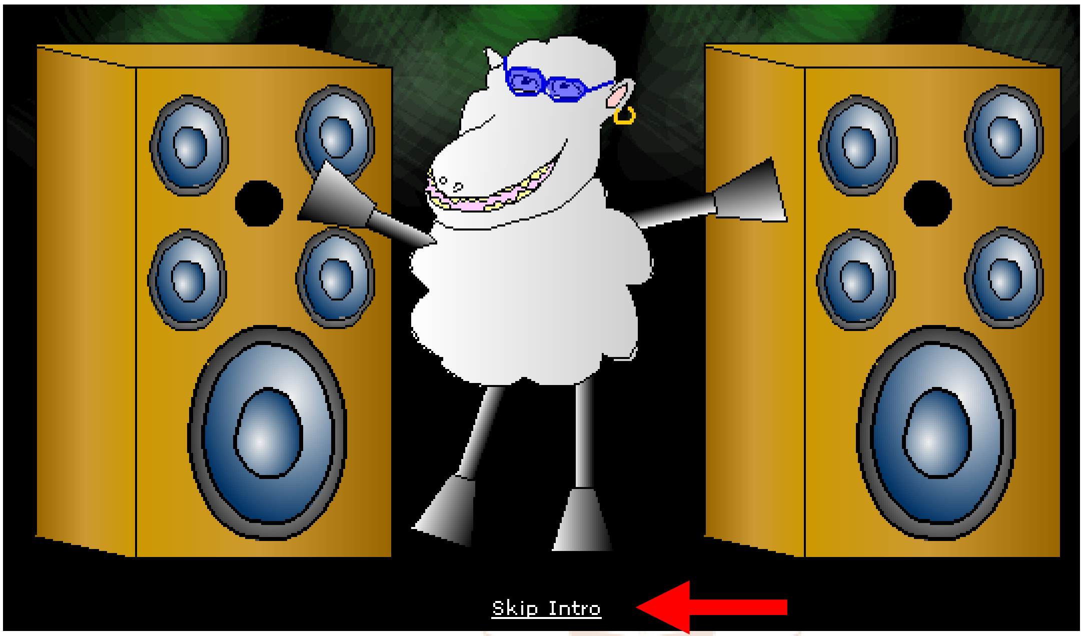
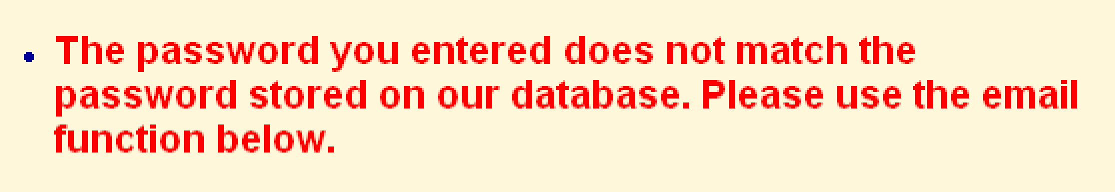


Fig 7.9 Skip Intro

7.4.5 Help users recognise, diagnose and recover from errors

Error messages need to convey to the user whether the error is a security error on the page or just a standard web error. The user also needs to be told what action should take if there is an error while surfing a website. For example, is there a telephone number the user can dial for assistance? This is particularly important if a web page crashes during a transaction and the user is left wondering if their details such as credit card number and shipping address are secure and whether the transaction was a success.

Figure 7.10 shows an example of an error message which is displayed when the user enters the correct email address but incorrect password.

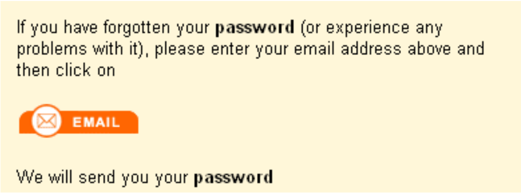


- **The password you entered does not match the password stored on our database. Please use the email function below.**

Fig 7.10 Incorrect password error message [KALA]

The error message is easy to understand, and tells the user exactly what has occurred. It also tells the user how to solve the problem by using the email function below (figure 7.11). The added usability of implying that the username is correct but the password is incorrect has a trade-off on the security of the site. This is because from a security point of view this error message makes the website more vulnerable to a brute force attack. The hacker now knows that the username is correct but the password is not. A solution to this is to make the message more ambiguous and state “The password/username combination entered is incorrect”.

Fig 7.11 Send password via email [KALA]



If you have forgotten your **password** (or experience any problems with it), please enter your email address above and then click on

We will send you your **password**

7.4.6 Satisfaction

On the Internet, compared to the brick and mortar world, it is normally very easy for a user to change their patronage from one company to another as a competitor’s website is only a mouse click away. It is therefore important for a website to ensure that their customers have at least a satisfactory online experience. Also, if the user is not satisfied with the level of security provided, they will go elsewhere.

In the next section it is seen how the implementation of the HCI-S criteria can lead to the development of trust.

7.5 HCI-S criteria lead to trust

As was seen in chapter 4, paragraph 4.3, the successful implementation of the HCI-S criteria will lead to the fostering of *Trust*. This is still true when it comes to interfaces found in an e-commerce environment. Two studies which confirm this are:

- eCommerce Trust Study by Cheskin Research and Studio Archetype/Sapient, 1999. This study included 463 web users; experts in the worlds of e-commerce, website development and academia [CHES99].

- Trust and the perception of security by InteractionArchitect.com, 2000. Research was focused on increasing the number of seats booked online for a major European airline [DHER00].

One of the main conclusions of both these studies is that trust online is not based solely on technical security features, but also on the user's feeling of control of the interactive system. If the operation of the website is flexible and predictable, then the user is more likely to *Trust* the website. During these studies users expressed comments such as:

> *"It [the interface] tells me what to do and it's clear even though I am not familiar with computers. I feel confident that I'll get what I want and that nothing strange will happen. I don't mind giving my credit card number in that case."* [DHER00]
>
> and
>
> *"I feel secure about giving my credit card number because it's [the interface] simple. I trust it because you see what you get. There is nothing hidden or obscure." [DHER00]*

The first quote states “It [the interface] tells me what to do ...”. The HC-S criterion of *Convey features* tells the user what features are available and then the criterion of *Learnability* ensures that the user is able to use the features.

In the second quote a user says “... because it's [the interface] simple.”. A website which has an *Aesthetic and minimalist design* is likely to be simple.

From the above points it can be seen that applying the HCI-S criteria in an e-commerce environment leads to the development of *Trust,* which means that the user is more likely to supply confidential information (such as credit card details). This may be a false sense of trust if the technology behind the interface is not adequate.

Trust either grows or diminishes for a user over time. The HCI-S of a website can be used to grow this trust.

There is a limit to the amount of trust which can be fostered just through an interface and the application of HCI-S criteria. Other factors such as the brand displayed on the website also have a major influence on the level of trust. Navigation around the website and the fulfilment of orders also play a crucial role in the development of trust. In the next section it is seen how brand, navigation and fulfilment influence trust and whether HCI-S principles have any relation to these three factors.

7.5.1 Brand, navigation and fulfilment

When a user visits an e-commerce site the brand, e.g. Amazon.com, is first noticed of the site. A brand which is already known by the user from the brick and mortar world, e.g. Pick 'n Pay, will obviously foster more trust online than an unknown brand. A user is more likely to trust www.picknpay.co.za because of the reputation Pick 'n Pay already has in the traditional shopping environment. This is seen in figure 4.3, chapter 4.

Once a user has noticed the brand they will begin to explore the site. This is where the navigation of the site becomes very important. Cheskin Research found that effective navigation is a prerequisite to the communication of trustworthiness to a user. If the navigation of a site is poor, it is very unlikely that a user will *Trust* the site [CHES99].

Once a user has navigated the site and found what they would like to purchase, they expect their order to be fulfilled successfully. In order to fulfil the order the correct process of selecting, packaging and shipping the order to the consumer needs to be followed. Providing a tracking number for their order, stating the user's consumer rights and what recourse can be taken if something goes wrong helps to ensure satisfactory fulfilment for the user.

Fulfilment viewed in isolation has little impact on the *Trust* in a website. However, if it is joined to effective navigation, then a website will be able to foster a high level of trust in its users [CHES99].

As shown in figure 7.12, effective navigation is the foundation for communicating trust to the users of a website. This means that by applying one of the HCI-S criteria, such as *Learnability,* to navigation the level of trust that a user has in a website can be increased. Effective fulfilment can then be built on top of this. If the company also has a well-known brand then the brand's reputation can also be used to add to the trustworthiness of a site [CHES99].

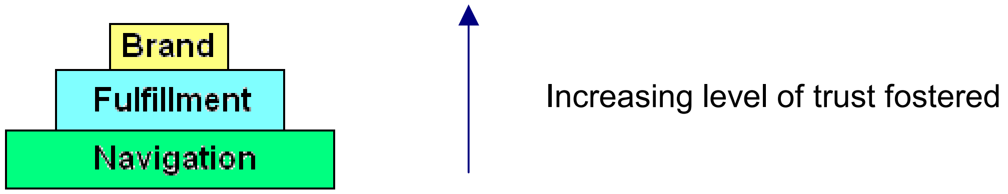
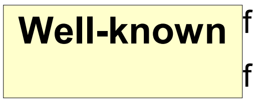


Fig 7.12 Components to establish trust

As long as effective navigation is one of two factors in place on a website, that site will be perceived by a user to be more trustworthy than a site which has one or none of these factors. A e-commerce site must have effective navigation if it wants to foster *Trust.* HCI principles can be used to improve navigation and fulfilment, leading to a more trustworthy website. Figure 7.13 shows how the six HCI-S criteria, along with other elements, can be used to enhance the trust which a user has in a website [CHES99].



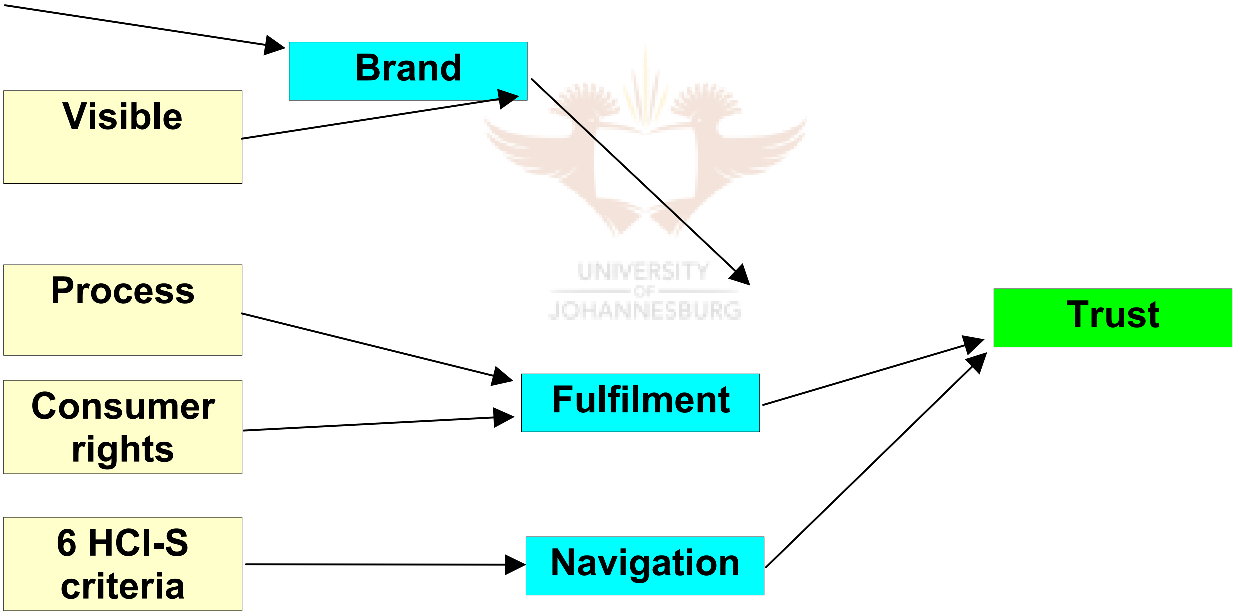


Fig 7.13 Enhancing the level of trust

7.5.2 Users' perceptions

Three quotes follow which help to articulate the points made on *trust:*

> *"Mature, well designed sites feel more stable and thus more trustworthy (not fly-by-night)."* Sean White, CTO of WhoWhere.com [CHES99]

> *"To a certain degree, the amount of "shlockiness" of a site -- its graphics, text, what's written, etc. -- the more I'd question it's trustworthiness if they asked me for card info."* Steve Glenn, CEO of Peoplelink.com [CHES99]

> *"A trustworthy site would be solid and no nonsense. It should feel sturdy and strongly branded. Design is a great way to communicate that. Consumers trust the design of "official looking" objects like money and legal documents and trust the feel of a bank."* Andrew Cramer, CEO of Online Partners.com Inc. [CHES99]

From these quotes it can be seen that a user's perception of security often has nothing to do with security features. This means that HCI-S principles are critical if a site wishes to convey trust and retain customers.

An important HCI principle is to "put the user in control". As was stated previously, this leads to increased *Trust*. A flexible and predictable interface helps the user maintain control over their online experience. In the next section the various components which make up a website are identified.

7.6 Functional security components of a website

The interface of a website is made up of various components. A component can be defined as a collection of code, for example HTML, server side code VB/Java script code, which when run forms an object which helps to make up a website. The user can normally see a component and sometimes interact with it. Examples of these components are menu bars, shopping carts, HTML links, graphics and buttons. All of these components influence the HCI of a website. However, the components are not always part of an HCI-S. A menu bar may be used to convey available security features or it may merely be used as a normal menu. The following six components have been chosen:

1. Registration
2. Passwords/login
3. SSL
4. Shopping carts and checkout
5. Logout button
6. Online help

The reason why these components have been chosen is that they are all involved in the generic process of purchasing an item online. A user first registers, then logs in using their password, adds items to their shopping cart and then proceeds to the checkout. The user is then able to logout. SSL helps to ensure the security of this whole process. Online help is also available to guide and assist the user throughout the process. Figure 7.14 shows this generic process.

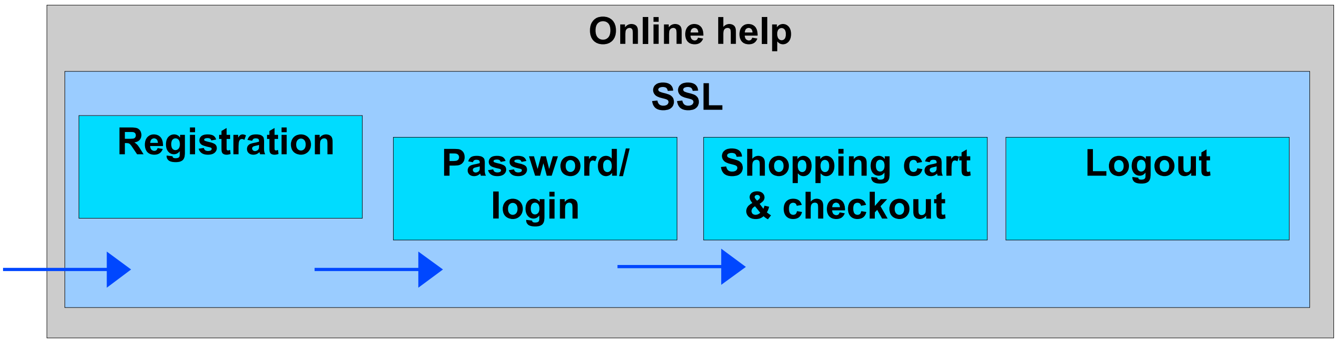


Fig 7.14 Generic online shopping process

Shopping carts and checkout and online help have also been selected because of their popularity and widespread use. This can be seen from the table below which shows 15 e-commerce sites. Sites have been chosen from the three broad categories of e-tailers, services and electronic banking. Each site was visited to determine which components were present. From the table it is obvious that the components of *registration, passwords, SSL, shopping carts & checkout* and *online help* form part of most web HCI-Ss.

Table 7.2 Components found in popular websites

	Registration	***Passwords/ login***	***SSL***	***Shopping cart & checkout***	***Logout button***	***Online help***
E-tailers						
Amazon.com	X	X	X	X		X
Dell.com	X	X	X	X		X
Ebay.com	X	X	X	X		X
Barnesandnoble.com	X	X	X	X		X
Officedepot.com	X	X	X	X		X
Kalahari.net	X	X	X	X		X
Woolworths.co.za	X	X	X	X		X
Picknpay.co.za	X	X	X	X	X	X
Digitalplanet.co.za	X	X	X	X		X
Services						
Sterkinekor.co.za	X	X	X			X
Computicket.co.za			X	X		X
Ibm.com	X	X	X	X		X

	Registration	*Passwords/ login*	*SSL*	*Shopping cart & checkout*	*Logout button*	*Online help*
Netflorist.co.za	X	X	X	X		X
Bidorbuy.co.za	X	X	X	X		X
Etravel.co.za			X			
Lastminute.com	X	X	X	X		X
Electronic banking						
ABSA.co.za		X	X		X	X
Nedbank.co.za		X	X		X	X
eBucks.com		X	X		X	X

In future chapters the above components found in websites are analysed according to HCI-S criteria. In the following paragraphs each component is discussed in more detail.

7.6.1 Registration

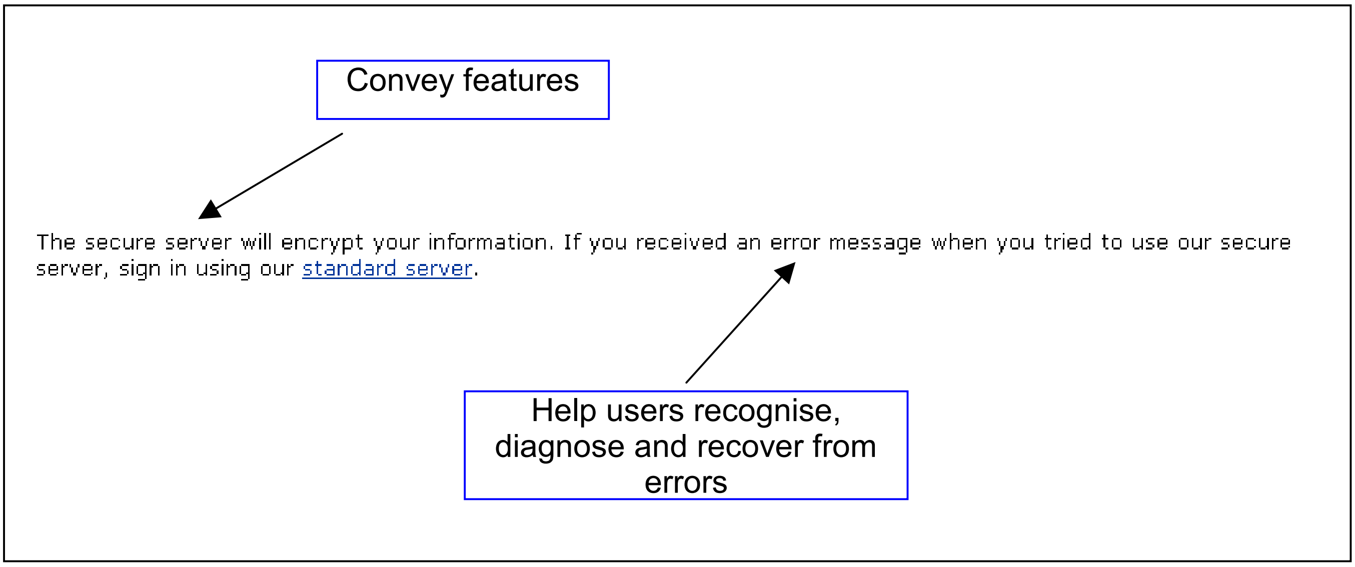
Many websites require users to register in order to use the site. This has its advantages as a more personal experience can be given to the user. It also saves the user from having to re-enter information (e.g. delivery address) when making a purchase. However, compulsory registration may sometimes be frustrating as a user may wish to purchase an item quickly. The user may also wish to retain a certain level of anonymity when shopping online. A registration process which asks for detailed personal information may discourage the user from using the site or may cause the user to enter invalid information.

During the registration process it is important for the user to feel in control. As was discussed in the previous section, allowing the user to feel in control while they are online will lead to an increased level of trust.

Jakob Nielsen [NIEL01], a usability expert, recommends letting the user use their email address as a user ID. The email address will be unique and the user is unlikely to forget it. Clear instructions need to be given throughout the registration process as some users expect their password to be emailed to them [NIEL01].

The interface only has limited control over the registration process. Many of the aspects of registration, for example the level of personal details required, are policy decisions which the company has made. The interface is merely implementing the policy. It is, however, important that the interface explain to the user exactly why registration is necessary, why the personal information is required and what the information will be used for. Policy decisions made by the owners of a website can have a huge impact on the usability of the site.

Figures 7.15 and 7.16 are two screen grabs taken from an online registration form. The relevant HCI-S criteria are identified by the blue boxes. An arrow from the blue boxes indicates where the criteria are relevant. However, not all the criteria, shown in the red boxes are directly addressed by the two screen grabs. An analysis of whether the HCI-S criteria have been met is not given at this stage.

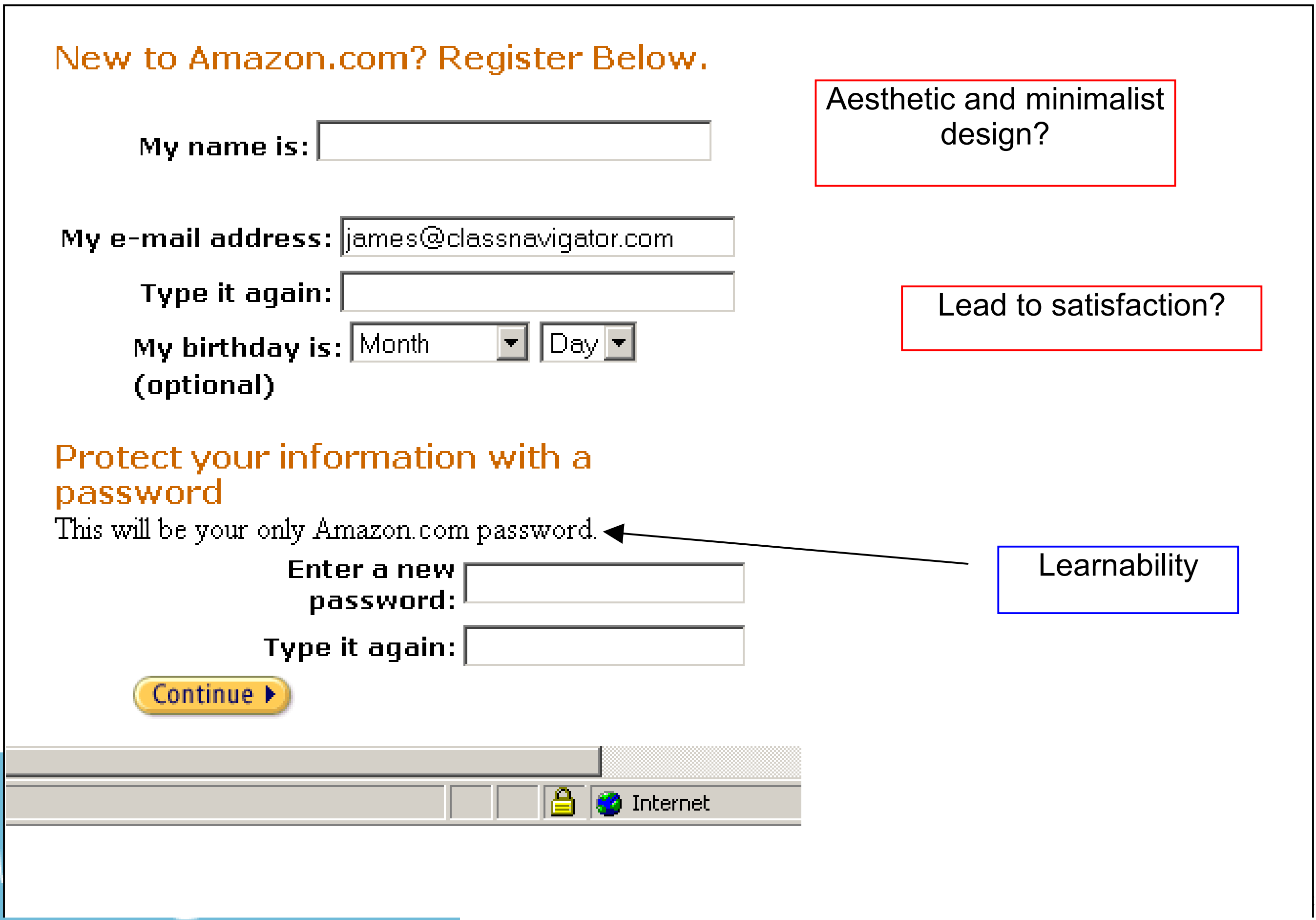


Convey features

The secure server will encrypt your information. If you received an error message when you tried to use our secure server, sign in using our standard server.

Help users recognise, diagnose and recover from errors

Fig 7.15 Registration Part 1 [AMAZ]



New to Amazon.com? Register Below.

My name is:

My e-mail address: james@classnavigator.com

Type it again:

My birthday is: Month Day
(optional)

Protect your information with a password

This will be your only Amazon.com password.

Enter a new password:

Type it again:

Aesthetic and minimalist design?

Lead to satisfaction?

Learnability

Visibility of system status

Fig 7.16 Registration Part 2 [AMAZ]

7.6.2 Passwords/login

A website assumes that a user is who they say they are based on the ability to provide the correct passwords. Retinal scanners, fingerprint readers and other biometrics will in the future be used as a form of identification and authentication. However, these techniques are not widely used yet. This means that currently passwords form the backbone of the IS service of authentication on the Internet.

Unauthorised access to systems, and the theft of information or the misuse of a system is often done by hackers 'cracking' user passwords, or obtaining them from the user by persuasion and deception. System security has sometimes been regarded as an entirely technical issue. However, the human factor cannot be ignored [ADAM97].

Passwords play a major role in an HCI-S. From an HCI and usability point of view some questions which should be asked are:

- How easy is the password to use?
- Is the password easy to lose or forget?
- Can the password be stolen or copied?
- How easy is it to change the password?
- Is the user informed of the policies and procedures with regard to passwords, e.g. is the password stored in an encrypted format on the server?

The aim of HCI-S is to make passwords and login as secure and usable as possible. Usability in the context of passwords can be defined in terms of how easy the password is to remember and the overheads involved in creating and using the passwords. Some passwords have overheads such as a limit to the length (e.g. 6-8 characters long) and content (e.g. only numbers) of the password. A password may also expire, and need to be reset over a certain time limit.

Some of the common myths about passwords are:

- Long passwords are more secure.
- A password chosen by the system is more secure.
- Forcing a password to be changed frequently leads to improved security.

From a security point of view the above myths appear to make sense, but from an HCI-S perspective they are counterproductive. Passwords based on these myths cause users to write down their passwords or even store them in a text file on their computer. In other cases the user is forced to change passwords frequently. The reason behind this is to reduce the risk associated with a compromised password being used. However, forcing a user to change a password frequently makes the password harder to remember. The user may write down the password, or choose passwords which are linked, for example bob1, bob2, bob3. In one study, 50% of the users surveyed admitted to writing down their passwords [ADAM99].

Windows also offers to remember a user's password, which could lead to a security breach.

The level of security provided by a username and password can vary greatly depending on the user's choice of password and their knowledge of security [ADAM97]. A possible solution is for a user to choose a short password which appears random. For example, a user could choose the initials of three best friends along with their birthdays. This type of password may be easier to crack, but the user is less likely to forget it. Another option would be to encourage the user to choose a pass phrase. A pass phrase is normally longer than a password and easier to remember. Clear instructions with regard to passwords need to be displayed by the interface. The content of possible instructions could be:

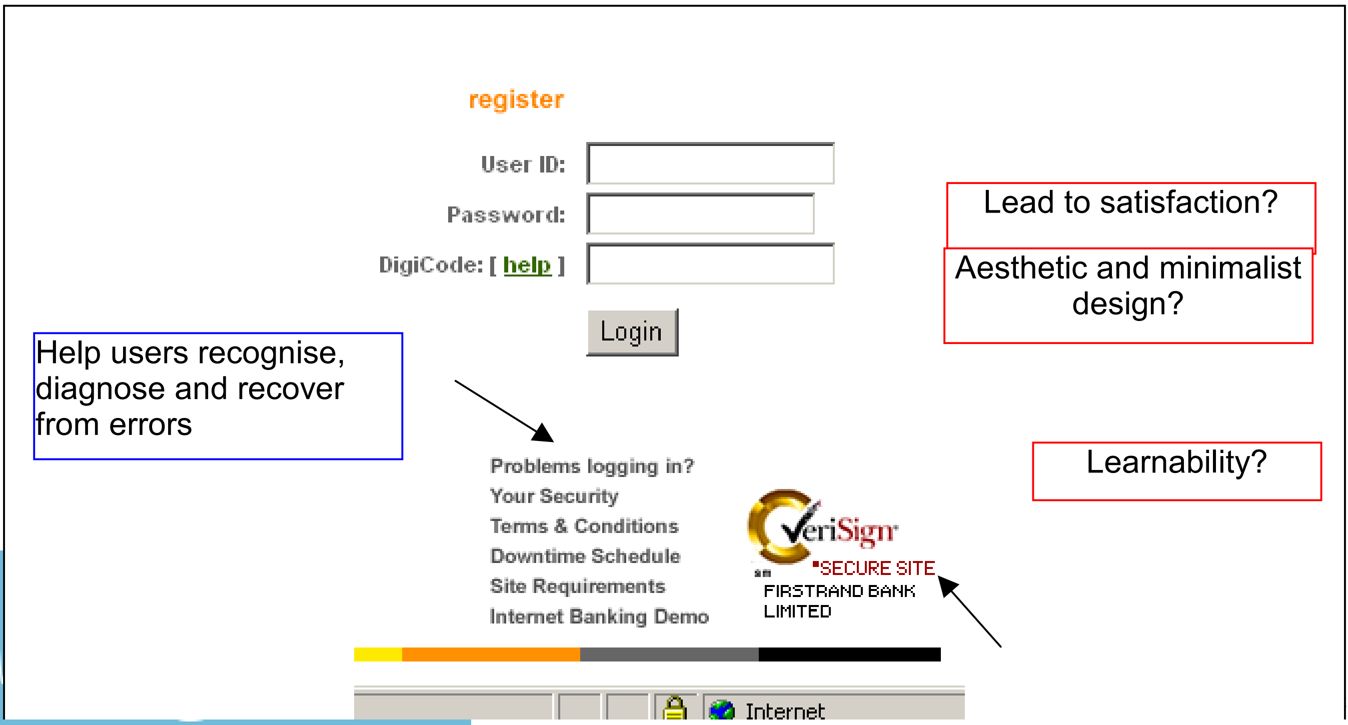
- The minimum and maximum length of the password.
- Whether the password is case-sensitive or not.
- Inform the user to choose a password that is not found in a dictionary.
- Ensure that the password contains numbers and symbols.
- Inform the user not to write the password down.
- Stress to the user the importance of keeping the password secret.
- Perhaps encourage the user to enter a pass phrase instead of a password, for example: 'IwasBornIn1983InJoburg'. The benefit of a pass phrase is that it is both memorable and secure.

A balance needs to be struck between a password that is relatively secure and one that is easy for the user to remember. If too much of a burden is placed on a user with regard to passwords, the user may rebel against the security policies and attempt to bypass them. A user could do this by sharing passwords with colleagues or by choosing 'password' for a password. As was seen in the component of registration, the policy of the business also affects the component of login/passwords. A policy of forcing the user to reset their password every month will negatively impact the usability of the site. A company will not be able to apply the HCI-S criteria without ensuring that their policies foster usability.

During the login process it is important for the user to be given guidance as to what to do if they have forgotten their username or password. One possible option, if the user has forgotten their password, is to email a new password. Another option is for the website to ask the user a number of questions, the answers to which they gave during registration. Correctly answering the questions results in the password being reset.

A recent addition to the password/login component is the introduction of graphical keypads and the use of pass phrases. These additions increase the security of the site but may negatively effect the usability of the login procedures.

The HCI-S criteria of *Convey features, Visibility of system status, Learnability, Aesthetic and minimalist design, Help users recognise diagnose and recover from errors* and *Satisfaction* relate to the login component. Figure 7.17 shows how some of the HCI-S criteria relate to a login page. As before, the criteria are in blue boxes.



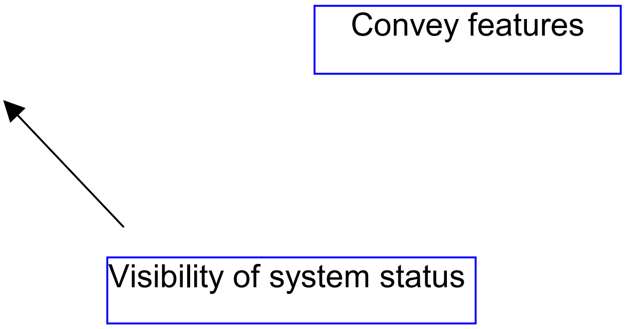


Fig 7.17 Login [EBUCKS]

7.6.3 SSL - secure connections

On the Internet the security pillars of authentication, integrity and confidentiality are implemented through the use of SSL. Sites which support SSL have 'https' instead of 'http' in their URL (figure 7.19). Internet Explorer also shows a 'padlock' icon (figure 7.18) in the bottom left-hand corner of the window when the connection is secure. Internet Explorer may also inform the user that they are now viewing pages over a secure connection (the user may have chosen to ignore any of these future warnings).

Fig 7.18 Padlock icon

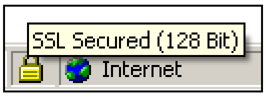
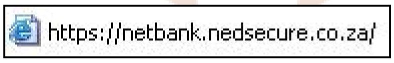

SSL Secured (128 Bit)
Internet

Fig 7.19 Site that supports SSL


https://netbank.nedsecure.co.za/

If users notice the padlock and https, they may not know what they mean. The designer of a website needs to take this into account and ensure that the user is made aware in a clear and concise manner of these security features.

During the SSL handshake the client browser generates a session key. This session key is encrypted with the server's public key and then sent to the server. The session key is then used by the browser and server to ensure that all information sent over the Internet is encrypted.

While SSL is being deployed at a website it is important for the HCI-S criteria of *Convey features, Visibility of system status* and *Satisfaction* to be met.

7.6.4 Logout button

When a user has entered a username and password and 'logged in' they expect also to be able to 'logout'. A 'logout' button displayed in a prominent position will aid the user in feeling secure. A site must also be able to handle users who do not logout.

Clicking on the logout button is very important as it ends the user's online session with a web server. This means that the user will have to login again if they want to use the site. Closing the browser window does not necessarily end the session and may leave the session more vulnerable to hijacking. It is also possible for another website to hijack a user's session if they visit the other website before logging out. Session hijacking is a where hacker takes over a session pretending to be the original user. The server is led to believe that it is communicating with the original user when it is actually dealing with the hacker. A user is normally only verified once when using a website, e.g. when they login. A session key is generated at login and passed between the user's browser and the server throughout the session. The session key may be stored in a cookie on the user's computer or passed in the URL. Clicking on the logout button should permanently end the session. This means that the user's session is no longer vulnerable even if a hacker managed to obtain the session key.

The user should also be reminded when they logout to clear the cache of their browser for an extra level of security.

The criteria of *Visibility of system status, Aesthetic and minimalist design, Help users recognise diagnose and recover from errors* and *Satisfaction* are relevant for logout buttons.

7.6.5 Shopping cart and checkout

This component is made up of the actual 'cart' where users electronically store their purchases and the payment process which they follow when they 'checkout' and purchase the items in their shopping cart. Users sometimes discard their shopping cart because the payment process is too long, complicated or the user feels insecure. The user is already at the site and has decided what to buy. An HCI-S which guides the user quickly and easily through a secure payment process will lead to satisfied customers who return [NORM01].

The shopping cart and checkout relate to security in that it is important to ensure that the transaction taking place during checkout is secure. The main reason why the shopping cart and checkout have been included as a component is that they play a crucial role in the development of trust. This is because the shopping cart and checkout form part of the navigation and fulfilment of a website, both of which are important when it comes to the development of trust. It is important for the user to feel in control of the shopping cart. The shopping cart must allow the user to easily add and remove products.

Some sites, for example Amazon.com, offer the ability to store the user's credit card details when they register. This aids the usability of the site as purchases can now be made in a shorter amount of time with fewer clicks. However, storing the user's credit card details can also be a huge security risk. A hacker may gain access to the credit card database, leading to financial losses and a total breakdown in trust between the company and their customers. The site could alternatively only ask the user for their credit card details when they purchase a product. The aim of the interface during the checkout process is to ensure that the user is at a point where they feel comfortable and trust the system so that they will provide their payment details.

The checkout process may also offer other payment methods, apart from credit cards. For example, the user may be able to pay by direct deposit, blue beans, eBucks or via icanonline. This provides the user with added flexibility and helps them to feel in control of the payment process.

The issue of confidentiality is also important with regard to the contents of the shopping cart. All six HCI-S criteria are relevant for the shopping cart and checkout components.

7.6.6 Online help

An important component of a website is the online help that is available to the user. Websites often have security features which use confusing technology (e.g. SSL). A help function is therefore necessary which explains these technologies in a way that is easy for the average user to understand. This helps to develop trust. The help also needs to be context-sensitive and must not be a nuisance to the user.

One effective and popular format for help is to have a question and answer page. There, frequently asked questions such as “Is online banking safe?” can be answered. The online help should guide the user through the process of making a purchase or using an electronic banking function.

In the next section the relationship between the above components and the HCI-S criteria is discussed.

7.7 Components supported by HCI-S criteria

Each of the components discussed in the previous section are supported by some or all of the HCI-S criteria. For example, the component of passwords/login is supported by all the HCI-S criteria. This means that if the component is found on a website it can be analysed according to the HCI-S criteria which relate to it. If a component is not supported by an HCI-S criterion, for example SSL is not supported by *Learnability*, then this means that the HCI-S criterion is not concerned with the component. Table 7.3 shows which HCI-S criteria support each of the components. A 'Yes' in a block indicates that the criterion supports the component, while a 'No' indicates that the criterion is not applicable to the specific component.

Table 7.3 Components supported by HCI-S criteria

HCI-S criteria ↓	*Registration*	*Use of passwords/login*	*SSL*	*Shopping cart & checkout*	*Logout button*	*Online help*
Convey features	Yes	Yes	Yes	Yes	No	Yes
Visibility of system status	Yes	Yes	Yes	Yes	Yes	No
Learnability	Yes	Yes	No	Yes	No	Yes
Aesthetic and minimalist design	Yes	Yes	Yes	Yes	Yes	Yes
Help users recognise, diagnose and recover from errors	Yes	Yes	No	Yes	Yes	No
Satisfaction	Yes	Yes	Yes	Yes	Yes	Yes

HCI-S is important in the web environment. This is evident from table 7.3 which indicates that most of the HCI-S criteria are relevant for each web component.

In chapters 8 and 9 websites which contain the above components are analysed according to their corresponding HCI-S criteria.

7.8 Conclusion

At the beginning of this chapter background information was given on HCI in a web environment and why HCI principles are so important when it comes to websites. Based on this information the first objective of this chapter has been met. The second objective of this chapter, which was to update the HCI-S criteria so that they are web-focused, has been achieved by relating the HCI-S criteria to interfaces found on the Internet. The final objective has been met by the identification of components found on websites which form part of an HCI-S. The relationship between these components and the HCI-S criteria was also established. The goal of this chapter, which was to develop the HCI-S criteria further so that they may be used to analyse security interfaces found in an e-commerce environment, has therefore been achieved.

HCI-S aims to minimise the relative amount of illegal use of a system while still maintaining a user-friendly interface. A method to do this is to identify each of the components on a website and to analyse them according to the relevant HCI-S criteria.

This chapter has shown that the HCI-S criteria are relevant in a web environment. As was seen, some additional aspects of each criterion need to be taken into consideration in an online environment. This means that the HCI-S criteria can be used to analyse and develop interfaces in both an online and traditional software environment.

In a traditional software environment the six HCI-S criteria are sufficient to foster trust. However, it is more difficult to develop trust in an e-commerce web environment. Fulfilment, brand and navigation, over and above the HCI-S criteria, also play an important role in the development of trust. The HCI-S assists the navigation of a site, thus helping to increase the level of trust.

In the next two chapters, six websites where security is important are evaluated using this method.

Chapter 8
Evaluation of Banking Websites

8.1 Introduction

"Things should be made as simple as possible -- but no simpler."
- A. Einstein

The HCI-S on an Internet banking site is crucial because financial losses are possible. Clients will only use the online banking service if they trust the system and feel confident enough in how to operate the site using the interface.

Online banking sites also need to be quick to use and content streamlined as they are used regularly by a client. The right balance needs to be met between a first-time user and an advanced user. A first-time user needs to be guided while the advanced user does not want to be hindered.

Worldwide, the use of Internet banking is growing. In the US it is predicted that by 2010, 55 million US households will use online banking services [EPAY01]. In South Africa 43% of Internet users use online banking [BIM00]. However, the main reason why some people have stopped using online banking is that they 'didn't understand the system' (table 8.1). This reason can be solved by applying HCI-S principles.

Table 8.1 Reasons why people stopped using online banking [EPAY01]

Reason	Total
Didn't understand system	33%
Payment problems	25%
No value	13%
Inconvenient	11%
Other	18%

The aim of this chapter is to use the HCI-S criteria to calculate the level of trust which various online banking websites foster. In order to achieve this aim three objectives need to be met. The first objective is to use the HCI-S criteria to analyse the components found on three banking websites. Once the interfaces have been analysed, the second objective is to attempt to quantify the level of trust which each interface fosters using the same method employed in chapter 5. The third objective is to attempt to identify the reasons why certain banking interfaces foster a higher level of trust than others.

In the previous chapter, the various components which form part of the interface found in an e-commerce environment were discussed. The HCI-S criteria (chapter 4) were also modified and added to so as to better suit the Web. Three banks – ABSA, Nedbank and First National Bank (FNB) – have been chosen. The reason for choosing these three banks is that they, along with Standard Bank, are the four largest commercial banks in South Africa [NED301]. ABSA's online banking site can be found at www.absa.co.za, and the Nedbank site is called NetBank.co.za. First National Bank's online site can be found at eBucks.com.

This chapter is lengthy due to the large number of screen grabs and tables. It has therefore been divided into three sections:

- Section A – Analysis and recommendations for Nedbank
- Section B – Analysis and recommendations for eBucks
- Section C – Analysis and recommendations for ABSA

8.2 Components used

In the previous chapter it was seen that the security interface of a website is made up of various components:

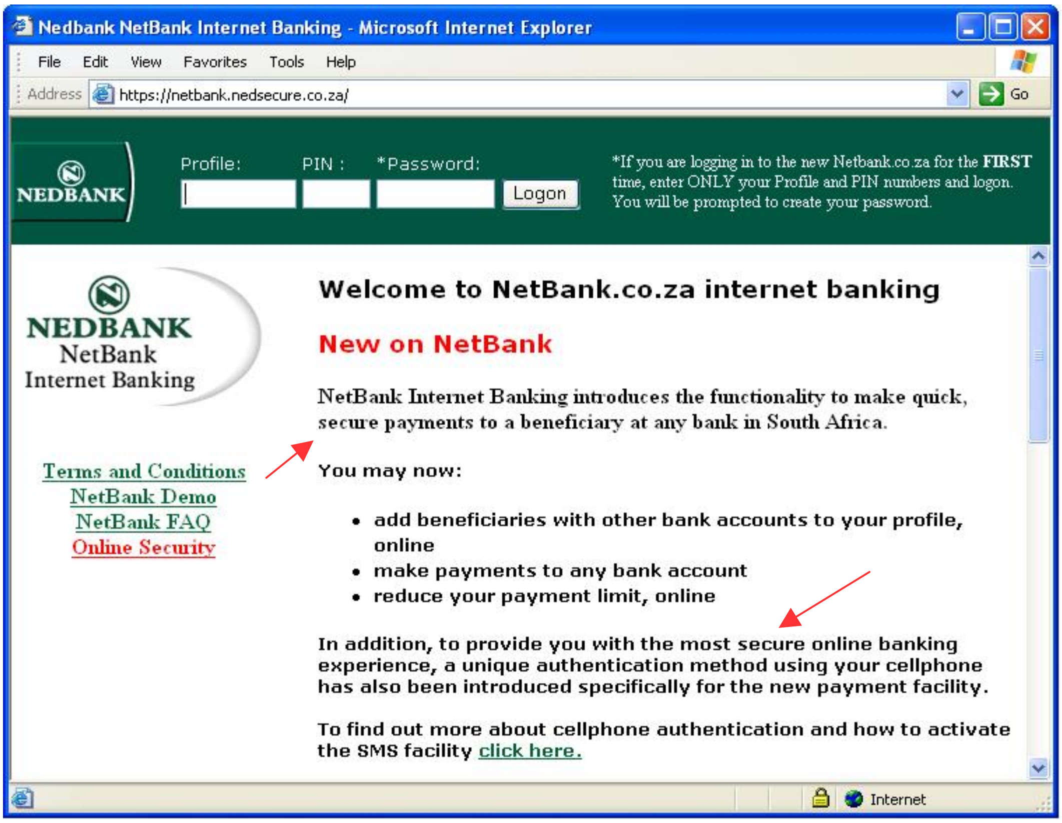
- Registration
- Passwords/login
- SSL – secure connections
- Shopping cart
- Logout button
- Online help

The components of passwords/login, SSL, logout button and online help are relevant to most banking sites. Components such as the shopping cart are used mainly by e-commerce sites and not by banking websites. These components, found on the ABSA, Nedbank and FNB sites, will be analysed according to the HCI-S criteria.

SECTION A

8.3 Analysis of NetBank.co.za

NetBank is the online banking portal for Nedbank. According to Nedbank, NetBank.co.za "introduces the functionality to make quick, secure payments to a beneficiary at any bank in South Africa" [NED02].


Nedbank NetBank Internet Banking - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://netbank.nedsecure.co.za/
Go
NEDBANK
Profile:
PIN :
*Password:
Logon
NEDBANK
NetBank
Internet Banking
Terms and Conditions
NetBank Demo
NetBank FAQ
Online Security
Internet

*If you are logging in to the new Netbank.co.za for the **FIRST** time, enter ONLY your Profile and PIN numbers and logon. You will be prompted to create your password.

Welcome to NetBank.co.za internet banking

New on NetBank

NetBank Internet Banking introduces the functionality to make quick, secure payments to a beneficiary at any bank in South Africa.

You may now:

- add beneficiaries with other bank accounts to your profile, online
- make payments to any bank account
- reduce your payment limit, online

In addition, to provide you with the most secure online banking experience, a unique authentication method using your cellphone has also been introduced specifically for the new payment facility.

To find out more about cellphone authentication and how to activate the SMS facility click here.

Fig 8.1 NetBank home page

NetBank's welcome screen has a simple and uncluttered look (figure 8.1). The user is able to login immediately by using the login bar at the top of the page. The welcome screen also assures the user of the security of the site, which will assist the user in trusting the system. The 'https' in the URL and the padlock in the bottom right-hand corner of the browser window also alert the user to the fact that the connection is now secure. The 'https' and padlock can, however, be easily missed by the user.

The user is also informed that their banking experience can be made even more secure by using a cell phone authentication method. In order to take advantage of this extra authentication the user needs to register their cell phone number in person at a branch.

This enables a confirmation code to be SMSed to the user's cell phone during Internet banking. Transactions cannot be completed unless this SMS confirmation code is entered. These features will assist the user in trusting NetBank. However, if a user does not have a cell phone, their banking functions will be severely limited. The user will only be able to make once-off payments of up to R1 000. Beneficiaries will need to be added at a branch.

8.3.1 Passwords and login

NetBank uses a PIN and a password, shown in figure 8.2. Both are chosen by the user. This adds to the *Learnability* of the website, as the user can choose a password and PIN which is easy for them to remember. Using two passwords may also increase the user's trust. NetBank has focused on an *Aesthetic and minimalist design* which is quick to download.

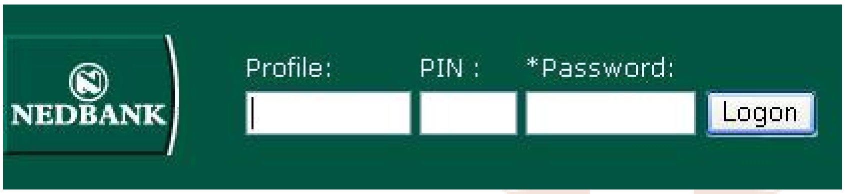
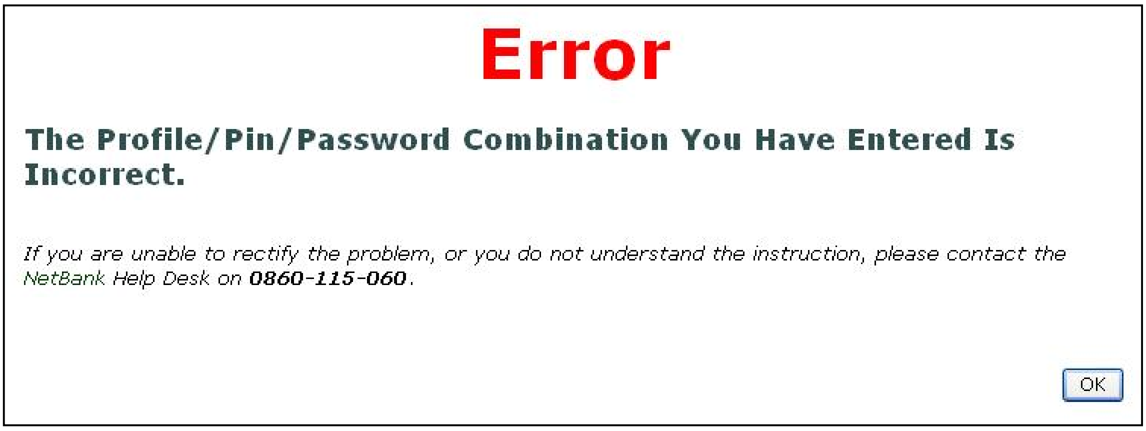


Fig 8.2 Login - NetBank

NetBank uses the term 'profile' instead of 'username'. This is because a profile number is assigned to each client who uses Internet banking. A company may have one bank account to which three employees have access. Each employee has their own profile number and can have different access rights. For example, one employee may be able to transfer funds while another is only able to check the account balance. The user is not able to choose or change the profile number. Perhaps it would have been better if NetBank had used the more familiar terminology of 'username' instead of 'profile' and allowed the user to choose their own username. This would mean one less number that the client needs to remember and would aid the flexibility of the site and help the user to feel in control of their browsing experience. An example of a banking site which uses usernames is icanonline.co.za. Letting the user choose a username does, however, have the disadvantage in that the user's preferred username may already have been taken, forcing the user to choose a new username which may be easily forgotten.

When a user logs on to NetBank they are not informed of the date and time of their last login. A user who is familiar with other banking websites would expect this information.

Providing this information could have helped to increase the level of trust.



Error

The Profile/Pin/Password Combination You Have Entered Is Incorrect.

If you are unable to rectify the problem, or you do not understand the instruction, please contact the NetBank Help Desk on **0860-115-060**.

Fig 8.3 Error message - NetBank

The error in figure 8.3 occurs when the user enters the incorrect password or profile number. This error message is a bit harsh and will probably give the user a fright the first time they see it. It is not very *Aesthetic* but does offer the client a way to solve the problem by advising the user to phone the help desk. This type of error message does not add to the user's enjoyment and *Satisfaction* of using the online banking facility.

A possible replacement for this error message could firstly be more specific as to whether the error is with the profile number or with the PIN or password. This trade-off in security would aid the usability of the login process. Secondly, some more general help could be given, such as asking the user to check if the Caps Lock key is active. Wording of a proposed error message is shown in figure 8.4:

Invalid Pin or Password

The Pin or Password you have entered is incorrect.

Try the following hints: * Is the "Caps Lock" or "A" light on your keyboard on?
If so, hit "Caps Lock" key before trying again.

* Did you forget or misspell your ID or password?
* The Pin contains only numbers while your password may be a combination of both numbers and letters.

* Please contact the NetBank Help Desk on 0860-115-060 for further assistance." [YAHOO]

Fig 8.4 Proposed error message

8.3.2 SSL – secure connections

NetBank uses 128-bit encryption. This means that there are about a trillion, doubled over and over on itself 88 times, different possible key combinations to decrypt the transaction. It would take significantly longer than the age of the universe to crack a 128-bit key [9DOLL]. This is extremely secure. On the welcome page the user is informed that the site is secure (figure 8.1).

The 'https' in the URL and the padlock in the bottom left part of the browser show that the site is secure. It is easy for a user not to notice these items, and if they do notice them, they probably won't understand them. The 'https' and the padlock are explained in the online help, but it would have been better to have had a full explanation of these security features on the welcome page (figure 8.1).

8.3.3 Logout/logoff button

Once a user has logged on a 'logoff button' is clearly displayed in the top right-hand corner (figure 8.5).

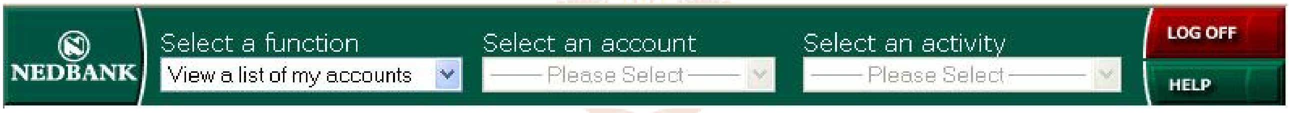
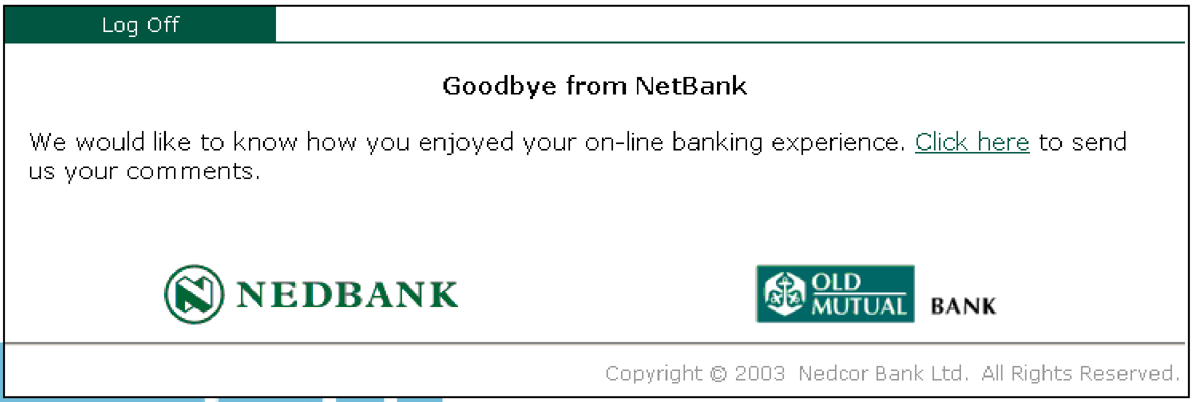


Fig 8.5 Logout and help buttons - NetBank

A logoff button helps with the *Visibility of system status*. From a banking point of view it is important for a user to log out once they have finished banking. After 8 minutes of not being active a user is automatically logged out. The importance of logging off is not conveyed to the user. The user is also not reminded to log off when they are finished. A message such as “Remember to click 'Logoff' when you are finished!” could be displayed on each page. This would encourage users to follow the good security practice of logging off.

When a user logs off, the screen in figure 8.6 is shown.



Log Off

Goodbye from NetBank

We would like to know how you enjoyed your on-line banking experience. Click here to send us your comments.

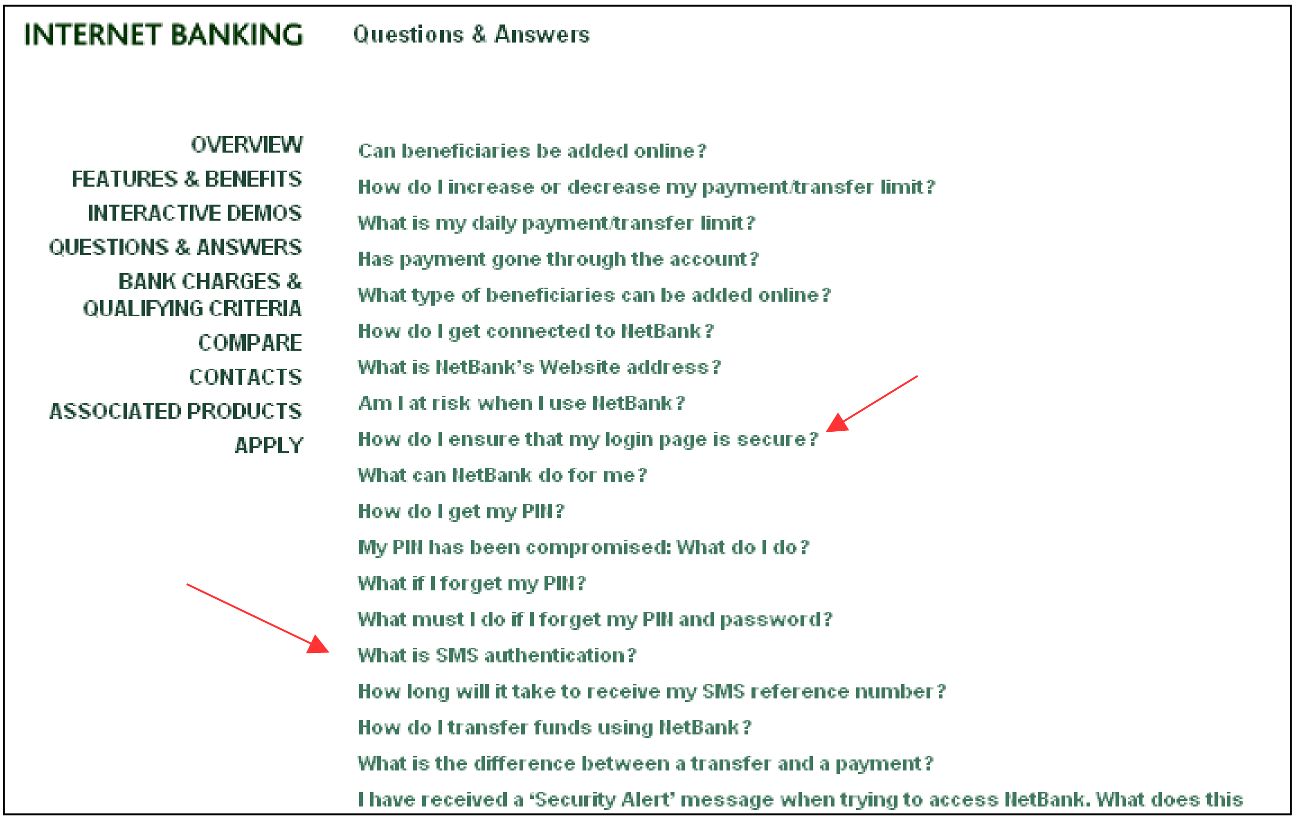
Copyright © 2003 Nedcor Bank Ltd. All Rights Reserved.

Fig 8.6 Logoff screen

Figure 8.6 has an *Aesthetic and minimalist design*. It also asks the user for feedback on their Internet banking experience. This will help to foster trust as it shows the user that Nedbank is interested in each client personally.

8.3.4 Online help

NetBank offers a comprehensive online help along with a frequently asked questions page. The frequently asked questions page is shown in figure 8.7, which helps to *convey* the available *security features.*



INTERNET BANKING Questions & Answers

OVERVIEW
FEATURES & BENEFITS
INTERACTIVE DEMOS
QUESTIONS & ANSWERS
BANK CHARGES & QUALIFYING CRITERIA
COMPARE
CONTACTS
ASSOCIATED PRODUCTS
APPLY

Can beneficiaries be added online?
How do I increase or decrease my payment/transfer limit?
What is my daily payment/transfer limit?
Has payment gone through the account?
What type of beneficiaries can be added online?
How do I get connected to NetBank?
What is NetBank's Website address?
Am I at risk when I use NetBank?
How do I ensure that my login page is secure?
What can NetBank do for me?
How do I get my PIN?
My PIN has been compromised: What do I do?
What if I forget my PIN?
What must I do if I forget my PIN and password?
What is SMS authentication?
How long will it take to receive my SMS reference number?
How do I transfer funds using NetBank?
What is the difference between a transfer and a payment?
I have received a 'Security Alert' message when trying to access NetBank. What does this

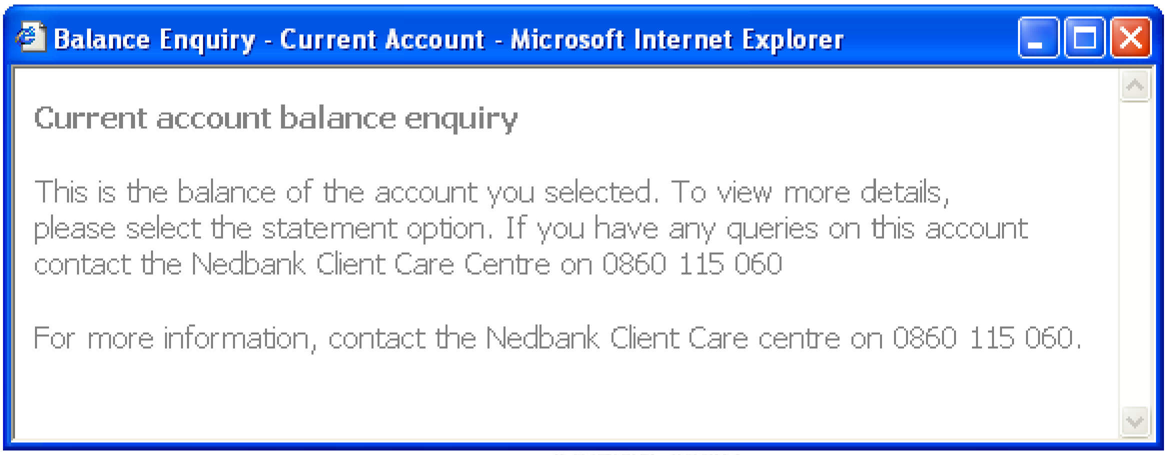
Fig 8.7 Help - NetBank

The online help assists the user in trusting the system as the user's questions and concerns can be answered quickly.

The online help does not contain a lot of technical jargon. Explanations like "leaving your computer unattended while you still have access to your banking details is much like leaving your wallet on your desk and gives unauthorised people access" are used [NED202]. This means that it is easier for a user to *learn* how to use the site.

The online help also *Conveys security features* in an easily understood manner and has an *Aesthetic and minimalist design.* The help is also context-sensitive, which means that clicking on the help button (figure 8.5) brings up help that is relevant to what the user is doing. The user is always able to phone the help line if necessary.

The help, however, is not very flexible. Clicking on the 'Help' button only brings up help on the functions which are currently being used. For example, if the user is currently viewing a 'Current Account Balance' then clicking on 'Help' will only bring up information on current accounts. It is not easy to view help on different topics as there is no search function or links available in the help (figure 8.8). This means that the navigation of help is severely limited.


Balance Enquiry - Current Account - Microsoft Internet Explorer

Current account balance enquiry

This is the balance of the account you selected. To view more details, please select the statement option. If you have any queries on this account contact the Nedbank Client Care Centre on 0860 115 060

For more information, contact the Nedbank Client Care centre on 0860 115 060.

Fig 8.8 NetBank context-sensitive help

A PDF help document which contains more detailed information is also provided. This may, however, be confusing as the 'help' is found in three places – FAQ page, PDF download and help page.

8.4 Conclusion of NetBank.co.za analysis

The summary of the analysis has been broken down into four tables – one for each component. The same method in paragraph 5.7 in which each HCI-S criterion is given a weighting will be used. An average percentage is calculated, based on the HCI-S weightings, for each criterion. This percentage is rounded up and reflects the level of trust.

An explanation of the colours found in the summaries is given in table 8.2. If an HCI-S criterion is not met, then 0 is added to the overall score for a component (red). Green means the criterion has been met and 100% of the weighting is added to the score. Orange is between green and red. In this case 50% of the possible weighting for a criterion is added to the score.

Table 8.2 Key

Colour	***Explanation***	***Influence on weighting***
Red	Criterion has not been met.	0% of weighting
Green	Criterion has been met.	100% of weighting
Orange	In some instances the criterion has been met, in other instances it has not.	50% of weighting
Gray	Criterion is not applicable for this component.	

Each criterion is given a weighting for each component of the website. For example, in the passwords/login component six criteria are used. This means that each criterion has a 16.6% weighting towards the trust score. 16.6% (per criterion) x 6 criteria = 100% total weighting.

8.4.1 Passwords/login

Table 8.3 summarises the analysis of the passwords/login component of NetBank.

Table 8.3 Passwords/login

Criteria	***Conclusion***	***Impact***	
Convey features (16.6% weighting)	**YES**	The user should feel confident logging in.	16.6%
Visibility of system status (16.6% weighting)	**NO** User is not informed of the date and time of last login.	Illegal access to a user's account may go unnoticed.	0%

Criteria	*Conclusion*	*Impact*	
Learnability (16.6% weighting)	**?** PIN and passwords are chosen by the user. Term 'profile' is used instead of 'account number'.	Some users may be confused by the term 'profile'.	8.3%
Aesthetic and minimalist design (16.6% weighting)	**YES** Login bar is found on Internet banking home page.	It is easy for a regular user to quickly login.	16.6%
Errors (16.6% weighting)	**Partial** Some of the error messages generated are confusing and intimidating.	A user may discontinue using the service because error messages are more severe than necessary.	8.3%
Satisfaction (16.6% weighting)	**Partial** It is not immediately obvious that the login was a success. The user is not greeted by name.	Login lacks personal touch.	8.3%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 58% level of trust has been developed.	**Total**	**58%**

A 58% level of trust is fostered during the login process. A user who logs in to a number of different websites may find the login process of NetBank particularly frustrating due to the extra password and the different terminology.

8.4.2 SSL

The SSL trust level is presented in table 8.4.

Table 8.4 SSL

Criteria	*Conclusion*	*Impact*	
Convey features (33.3% weighting)	**Partial** SSL feature is conveyed but not in detail. SSL is not mentioned on the home page of the banking site. A PDF help document can be downloaded with more information on encryption.	The user may not be aware that the connection is secure.	16.6%
Visibility of system status (33.3% weighting)	**Partial** The user is not informed that the connection is secure.	The user may not use the system.	16.6%

Criteria	*Conclusion*	*Impact*	
Learnability	Not applicable.	Not applicable.	
Aesthetic and minimalist design	Not applicable.	Not applicable.	
Errors	Not applicable.	Not applicable.	
Satisfaction (33.3% weighting)	**Partial** The user will probably not be aware that SSL is being used to ensure safe transactions.	Advanced users, or users who read the PDF file, will be satisfied that measures are being taken to encrypt communications.	16.6%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 50% level of trust has been developed.	**Total**	**50%**

The main reason for the low level of trust for the component of SSL is that it is not adequately explained. This could be particularly serious, as Internet Explorer 6.0 sometimes does not show a padlock in the bottom right-hand corner, even though a page is encrypted. The only way to see that the page is encrypted is to right click on the page and click ‘Properties’.

8.4.3 Logout button

Table 8.5 shows a summary of the logout button analysis.

Table 8.5 Logout button

Criteria	*Conclusion*	*Impact*	
Convey features (25% weighting)	**No** Importance of logging out is not highlighted. User is not encouraged to clear their temporary Internet cache on logout.	The user may not logout.	0%
Visibility of system status (25% weighting)	**Yes** A message is displayed which clearly states that the user has successfully logged out.	Clicking the logout button will help the user to feel confident that their banking session has ended.	25%
Learnability	Not applicable.	Not applicable.	

Criteria	Conclusion	Impact	
Aesthetic and minimalist design (25% weighting)	**Yes** Logout button is in a prominent position.	User should be able to locate the logout button quickly.	25%
Errors	An environment which generated errors could not be created.		
Satisfaction (25% weighting)	**Yes** The user's feedback is requested when they log off.	User will notice the personal touch.	25%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 75% level of trust has been developed.	**Total**	**75%**

NetBank scores highly in this component. The logout button is in a prominent position and the user is informed clearly whether they have logged out successfully. However, the importance of logging out is not highlighted.

8.4.4 Online help

The level of trust for the online help component is calculated in table 8.6.

Table 8.6 Online help

Criteria	Conclusion	Impact	
Convey features (25% weighting)	**Yes** Conveys features in an easy-to-understand manner. PDF can be downloaded which contains more detailed information.	Most users will understand the help provided.	25%
Visibility of system status	Not applicable.	Not applicable.	
Learnability (25% weighting)	**Yes** Context-sensitive help is provided. Frequently asked questions page is also provided.	Relevant help will probably be displayed for the user.	25%
Aesthetic and minimalist design (25% weighting)	**Partial** Help opens in own window. A user is not able to navigate from one help screen to another. Only context-sensitive help is given.	User may find the help frustrating to use.	12.5%
Errors	Not applicable.	Not applicable.	

Criteria	***Conclusion***	***Impact***	
Satisfaction (25% weighting)	**Partial** No navigation bar is provided in the help. User is only given context-sensitive help.	User will not be able to navigate help.	12.5%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 75% level of trust has been developed.	**Total**	**75%**

NetBank's help contains most of the necessary security information. However, the structure of the help is confusing.

Overall NetBank scores:

58%	login/passwords
50%	SSL
75%	logout button
75%	online help

giving an average level of trust of 65%.

This means that Nedbank's Internet banking website has met more than half of the HCI-S criteria. As can be seen from table 8.7, this score denotes an average interface.

Table 8.7 Description of scores

Overall score	***Description***	***Impact***
0%-49%	Inadequate interface	The user will avoid using the interface, which will lead to weak security.
50%-59%	Below average interface	The interface will confuse and frustrate the user.
60%-69%	Average interface	The user will tolerate the interface if they really need to use the program. They will become familiar with the interface over time.
70%-85%	Above average interface	Most of the interface will be easy to use. One or two aspects of the interface may irritate the user.

Overall score	***Description***	***Impact***
85%-100%	Excellent interface	The user will enjoy using the interface. The implementation of security features by the user is easy and intuitive.

The components of SSL and login/passwords scored poorly. A number of small changes could be made which would increase the level of trust for these two components. In the next section some recommendations will be made on how the level of trust can be raised by changing the interface.

8.5 Recommendations for NetBank.co.za

Recommendations based on the HCI-S criteria will be made for the four components of passwords/login, SSL, logout button and online help. A new level of trust will then be calculated which includes the recommendations. Recommendations will only be made for criteria which have not been met, or which were partially met.

8.5.1 Recommendations for passwords/login component

Recommendations according to the HCI-S criteria are given in the following table:

Table 8.8 Passwords/login

Criteria	***Recommendation***	***Conclusion after recommendation***	***Proposed score***
Convey features	Criterion has been met.		16.6%
Visibility of system status	Inform the user of the date and time of last login.	**Partial** System status is improved during login.	8.3%
Learnability	Allow the user to choose their own username.	**YES** A user who is familiar with web logins should be able to log in easily.	16.6%
Aesthetic and minimalist design	Criterion has been met.		16.6%

Criteria	*Recommendation*	*Conclusion after recommendation*	*Proposed score*
Errors	Change error message to proposed message (figure 8.4).	**YES** Error messages will not scare the user.	16.6%
Satisfaction	**Partial** Greet the user by name.	**Partial** User should enjoy the login process.	8.3%
Does the interface lead to trust being developed?			
Trust (100% weighting)	An 83% level of trust has been developed after recommendations.	**Total**	**Proposed: 83%** **Existing: 58%**

As can be seen from the above table, making a few modifications to the interface can lead to an increase in the level of trust from 58% to 83%. This means that users are more likely to use this component correctly and to have a satisfactory experience. These modifications are relatively inexpensive to implement and no new technology needs to be purchased.

8.5.2 Recommendations for SSL component

The level of trust with regard to the SSL component can be improved. The recommendations are given in the following table:

Table 8.9 SSL

Criteria	*Recommendation*	*Conclusion after recommendation*	*Proposed score*
Convey features	Reassure users on the home page that a secure technology - SSL - has been implemented.	**Yes** The user will realise that their connection is secure.	33.3%
Visibility of system status	Draw the user's attention to the small padlock. Perhaps request certification from a third party such as VeriSign.	**Yes** Users will login with confidence.	33.3%
Learnability	Not applicable.	Not applicable.	
Aesthetic and minimalist design	Not applicable.	Not applicable.	
Errors	Not applicable.	Not applicable.	

Criteria	*Recommendation*	*Conclusion after recommendation*	*Proposed score*
Satisfaction	User will be aware that measures are being taken to ensure the safety of their transaction.	**Partial** Users may not understand the technology but will be aware of its importance.	16.6%
Does the interface lead to trust being developed?			
Trust (100% weighting)	An 83% level of trust has been developed.	**Total**	**Proposed: 80%** **Existing: 50%**

Implementing the above recommendations should lead to an improvement in the level of trust. SSL is a powerful security component of which the user is often not aware. Implementing these recommendations will draw the user's attention to the use of SSL.

8.5.3 Recommendations for logout button component

The recommendations for the logout button component are summarised in table 8.10.

Table 8.10 Logout button

Criteria	*Recommendation*	*Conclusion after recommendation*	*Proposed score*
Convey features	Encourage user to logout on each page. Highlight the importance of logging out.	**Partial** Most users will logout correctly when ending their session.	12.2%
Visibility of system status	Criterion has been met.		25%
Learnability	Not applicable.	Not applicable.	
Aesthetic and minimalist design	Criterion has been met.		25%
Errors	An environment which generated errors could not be created.		
Satisfaction	Criterion has been met.		25%
Does the interface lead to trust being developed?			
Trust (100% weighting)	An 87% level of trust has been developed.	**Total**	**Proposed: 87%** **Existing: 75%**

The existing interface already meets three of the four applicable criteria. Reminding the user to logout will help to satisfy the criterion of *Convey features.*

8.5.4 Recommendations for online help component

Recommendations, along with a trust score for the proposed interface, are given in table 8.11.

Table 8.11 Online help

Criteria	***Recommendation***	***Conclusion after recommendation***	***Proposed score***
Convey features	Criterion has been met.		25%
Visibility of system status	Not applicable.	Not applicable.	
Learnability	Criterion has been met.		25%
Aesthetic and minimalist design	Place a navigation bar in the online help which allows the user to navigate from one help screen to another. Add a search feature where a user can search the help for assistance on a specific topic.	**Yes** User will be able to navigate the help and find the information they need.	25%
Errors	Not applicable.	Not applicable.	
Satisfaction	Use pictures and screen grabs to explain security features and principles.	**Partial** Concepts explained using graphics are easier to understand than when just explained in words.	12.5%
Does the interface lead to trust being developed?			
Trust (100% weighting)	An 88% level of trust has been developed.	**Total**	**Proposed: 88%** **Existing: 75%**

Adding a navigation bar to the online help will increase the usability of this component. The use of graphics and pictures could also be increased in order to convey the available features to users in an easily understandable manner. In table 8.12 the average trust scores are presented.

As can be seen from table 8.12, implementing the HCI-S criteria leads to the level of trust improving from 65% to 85%. An increase in the level of trust indicates an improvement in usability and in the probability of a user implementing security features correctly.

Table 8.12 Existing vs proposed interfaces

	Existing	***Proposed***
Login/passwords	58%	83%
SSL	50%	80%
Logout button	75%	87%
Online help	75%	88%
Average	**65%**	**85%**

In the next section the interface of eBucks.com (First National Bank) will be analysed.

SECTION B

8.6 Analysis of eBucks.com

eBucks.com is the replacement website for FirstOnline.co.za and forms part of First National Bank’s online presence. Along with Internet banking, eBucks.com also offers online shopping and the opportunity to earn and spend 'eBucks'.

eBucks.com's home page is shown in figure 8.9. It has an *Aesthetic and minimalist design* and a link is provided to 'Your Security'.

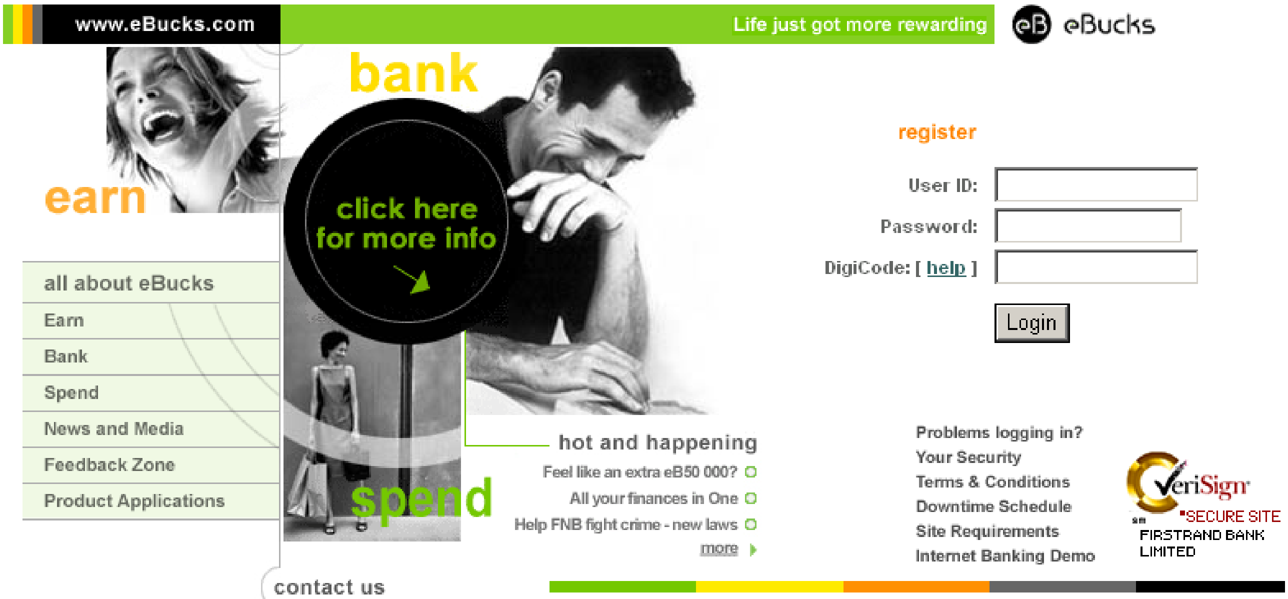
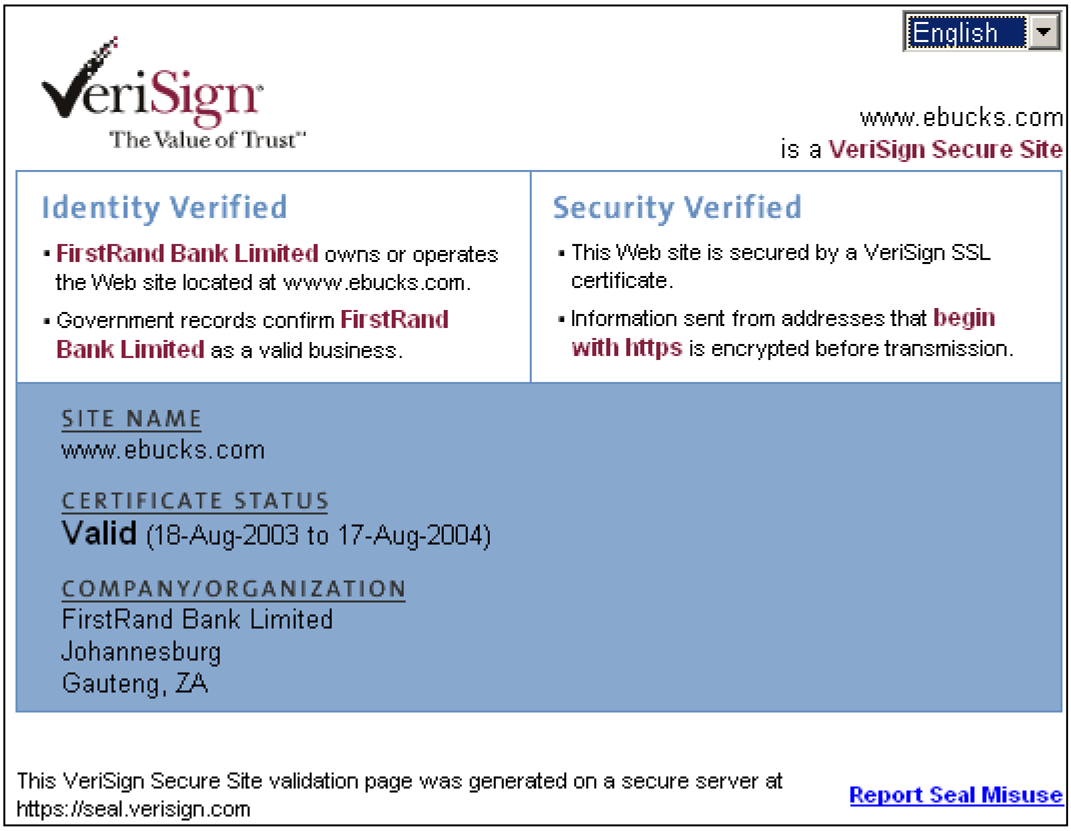


Fig 8.9 eBucks.com home page

A VeriSign logo is also present in the bottom right-hand corner. This is a third-party endorsement of the site and should help the user to trust the site. Clicking on the VeriSign logo allows the user to verify the identity of eBucks (figure 8.10). A website which displays the VeriSign logo indicates that a VeriSign certificate is being used to secure the site.



www.ebucks.com
is a VeriSign Secure Site

Identity Verified

- FirstRand Bank Limited owns or operates the Web site located at www.ebucks.com.
- Government records confirm FirstRand Bank Limited as a valid business.

Security Verified

- This Web site is secured by a VeriSign SSL certificate.
- Information sent from addresses that begin with https is encrypted before transmission.

SITE NAME
www.ebucks.com

CERTIFICATE STATUS
Valid (18-Aug-2003 to 17-Aug-2004)

COMPANY/ORGANIZATION
FirstRand Bank Limited
Johannesburg
Gauteng, ZA

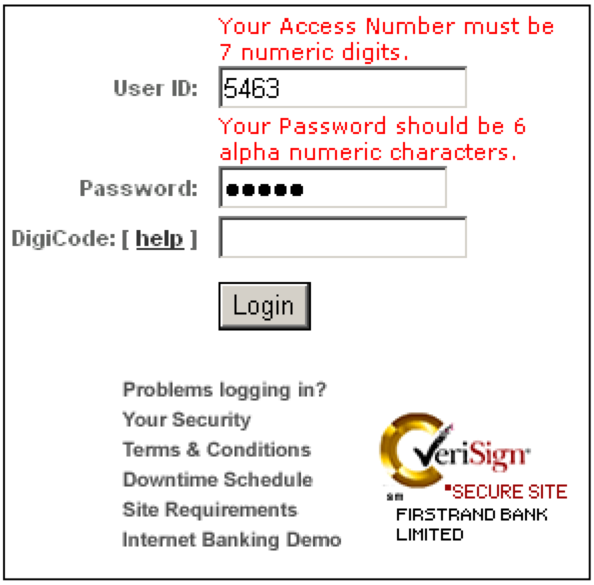
This VeriSign Secure Site validation page was generated on a secure server at https://seal.verisign.com

Fig 8.10 VeriSign verification [VERI04]

8.6.1 Passwords and login

Initially the login of eBucks.com had the potential to be confusing. The user was asked to enter a 7-digit access number in the User ID field. However, after contacting the eBucks.com help desk in March of 2003 it was determined that a 13-digit access number was actually required. The 7-digit access number was for users who migrated from FirstOnline.co.za. After the user had figured out what user ID or access number to enter, they would then need to enter their PIN in the Password field. The login of eBucks.com was not behaving in a predictable manner compared to other websites. This did not add to the *Satisfaction* of using the site. The error messages were also unclear. For example, the error message of "user ID minimum 8 characters" was obtained when a user ID/access number of the incorrect length was entered. This means that first the user was told 7 numbers and then 8 characters. During the course of this research most of these errors have been resolved. The login process is now less confusing. Users now have passwords instead of PINs, and the error messages have been fixed.

Figure 8.11 shows the current login found on the home page. A link to help is provided for any problems while logging in. Following this link provides contact information, helpful hints and the opportunity for a user to reset their password if the user knows the PIN for their ATM card.



Your Access Number must be 7 numeric digits.

User ID: 5463

Your Password should be 6 alpha numeric characters.

Password: ●●●●●

DigiCode: [help]

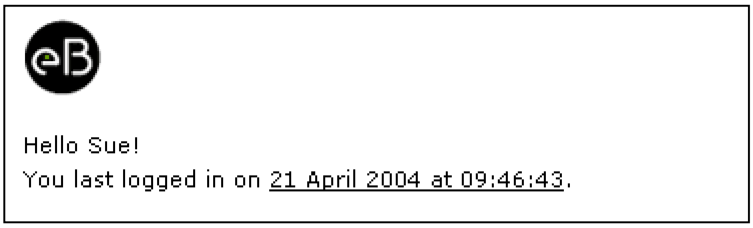
Fig 8.11 Login – eBucks.com

eBucks provides an additional level of security called a DigiTag. A DigiTag is a device which looks like a beeper. It has an LCD display on it which displays a list of unique "One-Time-Passwords" or DigiCodes. The DigiTag is synchronised with the eBucks server. If a user has a DigiTag they will need to enter a DigiCode along with their user ID and password. Having a DigiTag is not compulsory.

The error messages while logging in may be confusing. For example, if a user enters a password which is shorter than 6 characters and does not include numbers and letters, the following error is given: “Your Password should be 6 alpha numeric characters.” Users may not understand the term ‘alphanumeric’. If a user ID and password are given in the correct format but have incorrect values, the following messages is displayed: “Incorrect User ID or Password entered. Note: Access Details are case sensitive.” This reminds the user that they need to be careful with regard to the case of their username and password.

eBucks also provides an 'inContact' service through which the user is sent an SMS or email notifying them of any transactions on their account or logins to eBucks. However, the user is not informed of this on the login page.

After a successful login the user is welcomed by name (figure 8.12). They are also informed of the date and time of their last login. This will help to foster trust and the user will be able to see if their username and password has been compromised.



Hello Sue!
You last logged in on 21 April 2004 at 09:46:43.

Fig 8.12 Welcome

8.6.2 SSL – secure connections

As expected, eBucks uses SSL to encrypt all communication between the browser and server. However, no mention is made on the login page or transaction pages that the connection is secure. This means the *Visibility of system status* is not clear. An advanced user will notice that the page is secure by the 'https' and padlock. There is a link, however, to a comprehensive security guide which provides details and images about secure connections.

8.6.3 Logout button

A logout button is displayed in the top right-hand corner. It is quite small and easy to overlook.

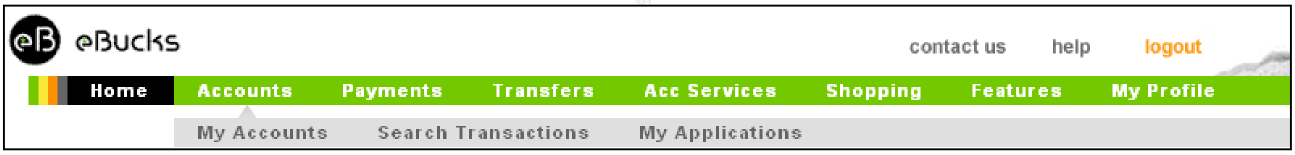
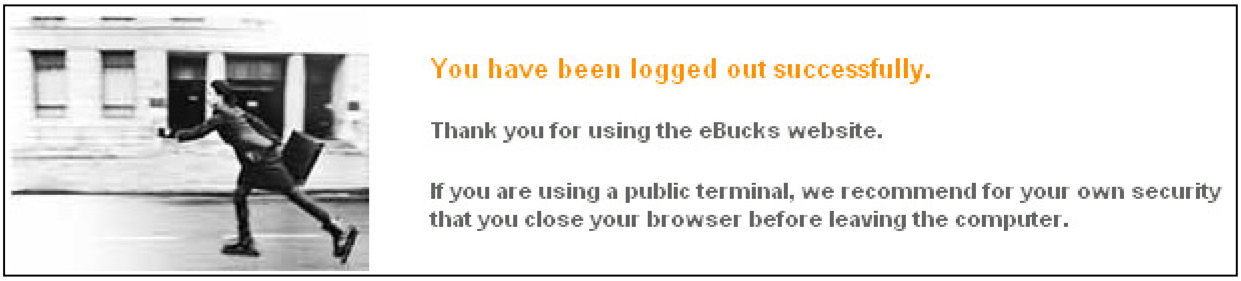


Fig 8.13 Logout button

After clicking the logout button the user is assured that the logout was successful. They are also thanked for using eBucks and encouraged to close their browser (figure 8.14).



You have been logged out successfully.

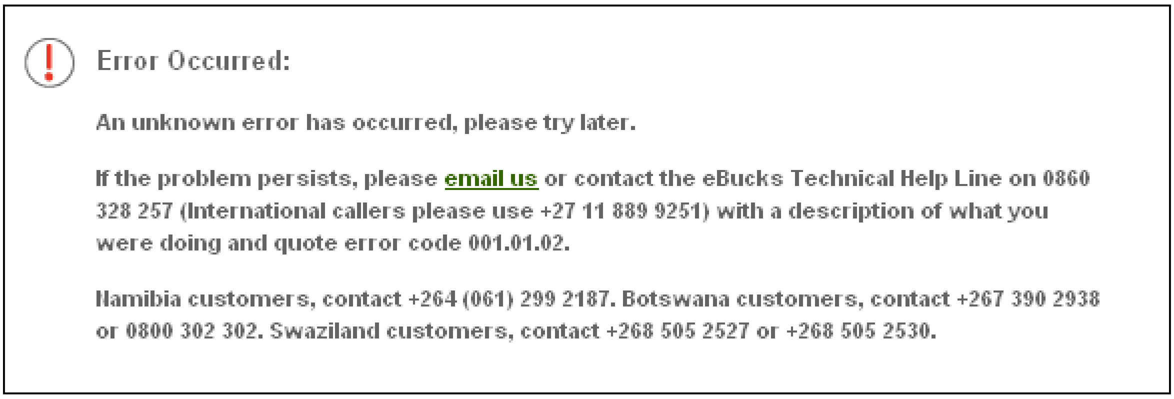
Thank you for using the eBucks website.

If you are using a public terminal, we recommend for your own security that you close your browser before leaving the computer.

Fig 8.14 Logout page

While using the site, the user is not reminded to logout when finished.

Error messages during logout are not specific. An example is shown in figure 8.15. Here the user is told that an 'unknown error' has occurred. The user is not told if it is serious, or if they can ignore it. Contact details are, however, given for assistance.



Error Occurred:

An unknown error has occurred, please try later.

If the problem persists, please email us or contact the eBucks Technical Help Line on 0860 328 257 (International callers please use +27 11 889 9251) with a description of what you were doing and quote error code 001.01.02.

Namibia customers, contact +264 (061) 299 2187. Botswana customers, contact +267 390 2938 or 0800 302 302. Swaziland customers, contact +268 505 2527 or +268 505 2530.

Fig 8.15 Error message - logout

8.6.4 Online help

eBucks.com offers an extensive help facility. The eBucks.com help offers detailed explanations of security features along with pictures. For example, figure 8.16 shows how to identify the padlock. Figure 8.17 shows how to check that the address in the URL is correct.

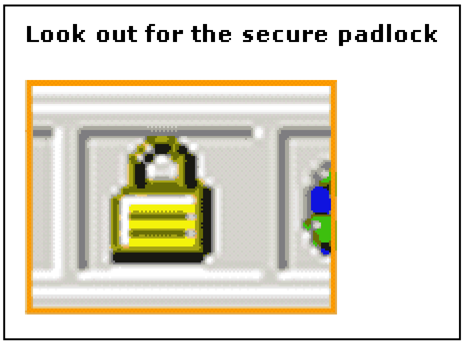


Fig 8.16 Online help – padlock

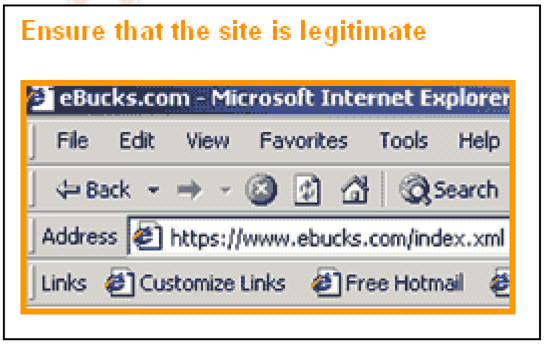

Ensure that the site is legitimate
eBucks.com - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search
Address https://www.ebucks.com/index.xml
Links Customize Links Free Hotmail

Fig 8.17 Online help - URL

Some of the other topics covered by the online help are:

1. Keep your bank card safe and your PIN secret
2. Keep your eBucks.com access details secret
3. Change your PIN and Password regularly
4. Don't allow your browser software to save or store your Password
5. Install and maintain the most credible anti-virus software
6. Shop securely online

Each topic is covered with simple and easily understandable explanations. For example, the following help is given about access details: *"Be particularly cautious when using public computer terminals - don't allow people to watch you typing in your information, and ensure that the browser does not store your password.*"

One topic which could be counterproductive is "Change your PIN and Password regularly". As was seen in chapter 7 (section 7.6.2) this could cause the user to write down their PIN and password. A user should rather be encouraged to choose a secure password and commit it to memory.

The help also deals with any known bugs in the browsers. For example, there is a bug in Internet Explorer which sometimes gives the following error message: *"This certificate has failed to verify for all of its intended purposes."* The user is advised by eBucks.com to ignore the above error message.

8.7 Conclusion of eBucks.com analysis

8.7.1 Passwords/login

Table 8.13 summarises the analysis of the passwords/login component of eBucks.com.

Table 8.13 Passwords/login

Criteria	***Conclusion***	***Impact***	
Convey features (16.6% weighting)	**YES** The user ID, password and DigiCode are all explained.	The user should feel confident logging in.	16.6%
Visibility of system status (16.6% weighting)	**YES** The user is told the date and time of last login.	User will be made aware of illegal access.	16.6%
Learnability (16.6% weighting)	**Partial** The term ‘User ID’ refers to the user's account number.	The user may be confused by terminology.	8.3%
Aesthetic and minimalist design (16.6% weighting)	**YES** Login bar is found on Internet banking home page.	It is easy for a regular user to quickly login.	16.6%
Errors (16.6% weighting)	**Partial** The meaning of the term ‘alphanumeric’ may be unclear to some users.	User may make unnecessary calls to the help desk.	8.3%

Criteria	*Conclusion*	*Impact*	
Satisfaction (16.6% weighting)	**YES** Use of the DigiTag could be particularly satisfying. The user is welcomed by name after a successful login.	User should be able to login quickly and easily.	16.6%
Does the interface lead to trust being developed?			
Trust (100% weighting)	An 83% level of trust has been developed.	**Total**	**83%**

An 83% level of trust is fostered during the login process. This is a high level of trust with most of the HCI-S criteria being satisfied.

8.7.2 SSL

A value of trust generated with regard to the SSL component is presented in the following table:

Table 8.14 SSL

Criteria	*Conclusion*	*Impact*	
Convey features (33.3% weighting)	**Yes** VeriSign Secure Site logo helps to convey to the user that security features are being used.	Users will trust eBucks.com because it has been verified by VeriSign.	33.3%
Visibility of system status (33.3% weighting)	**Partial** The user may not be aware that SSL is being used.	The user may not use the system.	16.6%
Learnability	Not applicable.	Not applicable.	
Aesthetic and minimalist design	Not applicable.	Not applicable.	
Errors	Not applicable.	Not applicable.	
Satisfaction (33.3% weighting)	**YES** If the user clicks on the VeriSign logo, they will be made aware of the security features. However, they are not reminded that the connection is secure.	User should feel confident using eBucks.com.	33.3%
Does the interface lead to trust being developed?			
Trust (100% weighting)	An 83% level of trust has been developed.	**Total**	**83%**

The level of trust which eBucks scores for this component is high. The main reason for this is the prominent use of the VeriSign Secure Site logo. The positive impact of using VeriSign will grow as more users become familiar with VeriSign.

8.7.3 Logout button

A summary of the logout button according to HCI-S criteria is shown in table 8.15.

Table 8.15 Logout button

Criteria	***Conclusion***	***Impact***	
Convey features (20% weighting)	**No** Importance of logging out is not highlighted. User is encouraged to close their browser, but they are not told to clear their temporary Internet cache.	User's session may be left open to hijacking.	0%
Visibility of system status (20% weighting)	**Yes** A message is displayed which clearly states that the user has successfully logged out.	Clicking the logout button will help the user to feel confident that their banking session has ended.	20%
Learnability	Not applicable.	Not applicable.	
Aesthetic and minimalist design (20% weighting)	**No** Logout button is not in a prominent position.	User may overlook the logout button.	0%
Errors (20% weighting)	**Partial** Error messages are not specific enough. They do, however, give contact details for additional assistance.	A user may be confused as to the severity of the error.	10%
Satisfaction (20% weighting)	**Partial** Logging out will not be a satisfying experience especially if an error message is displayed.	The user may avoid the logout button altogether.	10%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 40% level of trust has been developed.	**Total**	**40%**

eBucks scores poorly in this component. The main reason for this is that the importance of logging out, especially while using public computers, is not stressed. The potential error messages are also not clear, meaning a user may be left wondering if the logout was successful.

8.7.4 Online help

Table 8.16 shows a summary of the critical analysis of the online help component.

Table 8.16 Online help

Criteria	***Conclusion***	***Impact***	
Convey features (25% weighting)	**Yes** Features are explained in an easy-to-understand manner. Diagrams are used.	Most users will understand the help provided.	25%
Visibility of system status	Not applicable.	Not applicable.	
Learnability (25% weighting)	**Yes** Help is context-sensitive. Clear instructions are given. Help is broken up into logical sections.	Help is easy to use.	25%
Aesthetic and minimalist design (25% weighting)	**Yes** Navigation bar is given.	User will be able to navigate from one help topic to another. This also helps to encourage the user to 'explore' the help, thus improving the user's understanding of security.	25%
Errors	Not applicable.	Not applicable.	
Satisfaction (25% weighting)	**Yes** A user should find the help useful.	The discussion of topics such as anti-virus software will be beneficial to the user.	25%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 100% level of trust has been developed.	**Total**	**100%**

The online help of eBucks adequately satisfies all the applicable HCI-S criteria. This means that the online help will effectively assist the user to implement the various security features.

Overall eBucks scores:

83%	login/passwords
83%	SSL
40%	logout button
100%	online help

giving an average level of trust of 77%.

This means that eBucks has an above average interface with regard to security (see table 5.9). One or two aspects, particularly the logout button, could be modified in order to foster a higher level of trust.

8.8 Recommendations for eBucks.com

8.8.1 Recommendations for passwords/login

In table 8.17 recommendations are made on how the passwords/login component of eBucks.com can be improved with regard to the HCI-S criteria.

Table 8.17 Passwords/login

Criteria	***Recommendation***	***Conclusion after recommendation***	***Proposed score***
Convey features	Criterion has been met.		16.6%
Visibility of system status	Criterion has been met.		16.6%
Learnability	Provide an explanation for the term 'User ID'.	**Partial** User will understand that the user ID is their account number.	8.3%
Aesthetic and minimalist design	Criterion has been met.		16.6%
Errors (16.6% weighting)	Provide a more detailed error message for incorrect password or user ID.	**Yes** Most users will be able to understand the help message.	16.6%
Satisfaction	Criterion has been met.		16.6%
Does the interface lead to trust being developed?			
Trust	A 91% level of trust has been developed.	**Total**	**Proposed: 91%** **Existing: 83%**

The existing interface already fosters a high level of trust of 83%. This can be improved to 91% by making the error messages more user-friendly and providing an explanation of the term 'User ID'.

8.8.2 Recommendations for SSL component

Recommendations on how the SSL component can be improved from an HCI-S perspective are given in table 8.18.

Table 8.18 SSL

Criteria	***Recommendation***	***Conclusion after recommendation***	***Proposed score***
Convey features	Criterion has been met.		33.3%
Visibility of system status	Briefly mention the use of SSL on the home page.	**YES** The user will trust the system more because they will be aware that the connection is secure.	33.3%
Learnability	Not applicable.	Not applicable.	
Aesthetic and minimalist design	Not applicable.	Not applicable.	
Errors	Not applicable.	Not applicable.	
Satisfaction (33.3% weighting)	Criterion has been met.		33.3%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 100% level of trust has been developed.	**Total**	**Proposed: 100%** **Existing: 83%**

One small change to the interface – briefly mentioning SSL – can lead to the component of SSL meeting all the HCI-S criteria. A 100% level of trust does not indicate that the interface is completely perfect. It does mean that the user will be aware of this component and understand that it is an important security mechanism which should be implemented.

8.8.3 Logout button

Modifications to the logout button are proposed in table 8.19.

Table 8.19 Logout button

Criteria	***Recommendation***	***Conclusion after recommendation***	***Proposed score***
Convey features	On each page, encourage user to logout. Highlight the importance of logging out.	**Partial** Most users will logout correctly upon ending their session.	10%

Criteria	*Recommendation*	*Conclusion after recommendation*	*Proposed score*
Visibility of system status	Criterion has been met.		20%
Learnability	Not applicable.	Not applicable.	
Aesthetic and minimalist design	Increase the size of the logout button. Perhaps make it a stronger colour.	**YES** Users will be able to find the logout button more easily.	20%
Errors	Provide more specific error messages. Do not tell the user "An unknown error has occurred".	**YES** Most users will understand what action needs to be taken after an error message.	20%
Satisfaction	Logging out will be a satisfying experience.	**YES** Users will logout.	20%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 90% level of trust has been developed.	**Total**	**Proposed: 90%** **Existing: 40%**

The existing eBucks.com logout button scored poorly when analysed according to the HCI-S criteria. This component can be modified to satisfy the HCI-S criteria as shown in table 8.19.

8.8.4 Recommendations for online help component

Table 8.20 highlights the recommendations for the online help component.

Table 8.20 Online help

Criteria	*Recommendation*	*Conclusion after recommendation*	*Proposed score*
Convey features	Criterion has been met.		25%
Visibility of system status	Not applicable.	Not applicable.	
Learnability	Criterion has been met.		25%
Aesthetic and minimalist design	Criterion has been met. Perhaps increase the number of graphics used in the help.		25%
Errors	Not applicable.	Not applicable.	

Criteria	*Recommendation*	*Conclusion after recommendation*	*Proposed score*
Satisfaction	Criterion has been met. Perhaps include an online search feature.		25%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 100% level of trust has been developed.	**Total**	**Proposed: 100%** **Existing: 100%**

The existing online help component already meets all of the HCI-S criteria. It can, however, still be improved by adding more graphics and including a search facility.

Table 8.21 shows a comparison between the existing interface and the proposed interface.

Table 8.21 Overall score after recommendations

	Existing	*Proposed*
Login/passwords	83%	91%
SSL	83%	100%
Logout button	40%	90%
Online help	100%	100%
Average	**77%**	**95%**

From the above table it can be seen that implementing the HCI-S criteria can lead to an improvement of 18% in the level of trust.

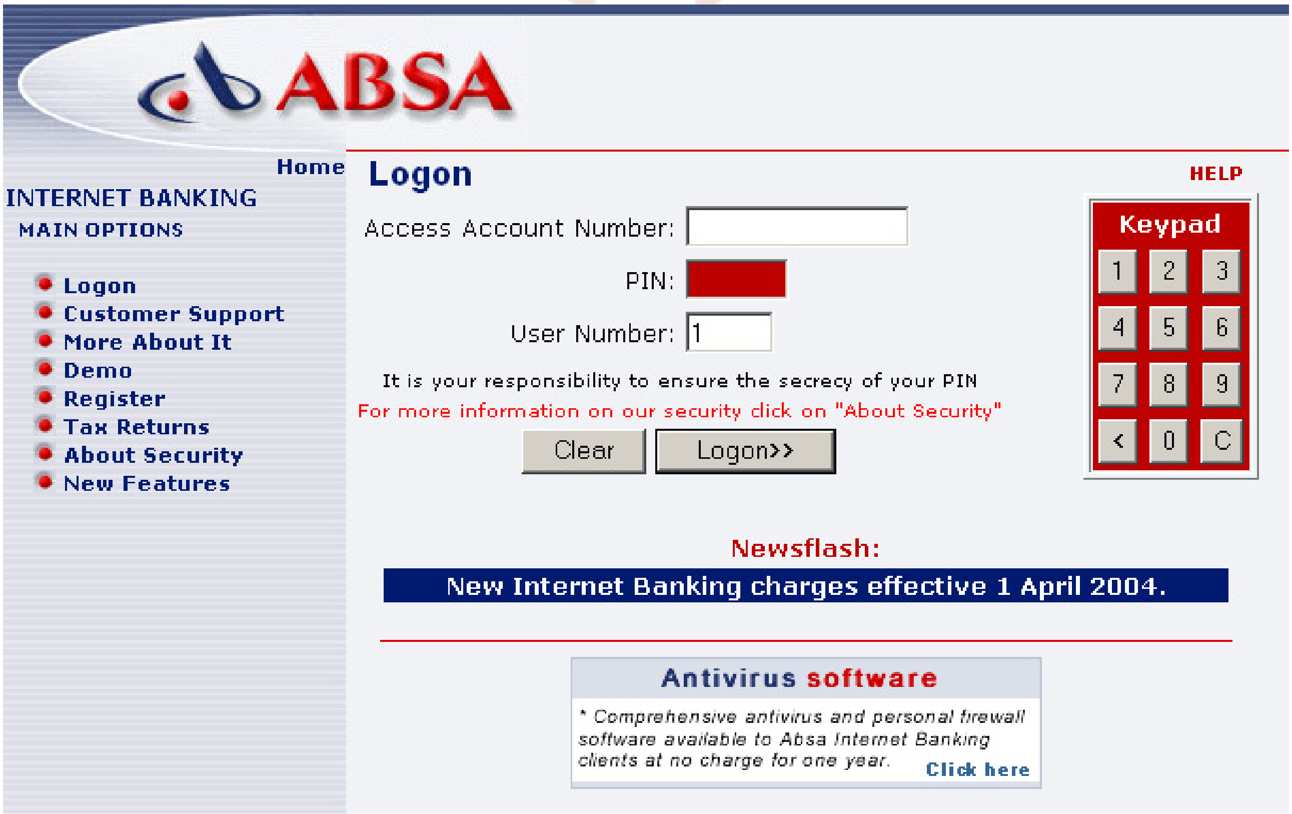
SECTION C

8.9 Analysis of ABSA.co.za

ABSA has over 400 000 users (2004) registered for online banking. This means ABSA has the largest number of online banking customers in South Africa. Each month Internet transactions worth over R17 billion are processed by ABSA. ABSA's dominance of the Internet banking market is set to continue with a 23% growth in new customers over the past year [WEIN04].

In June 2003 a number of ABSA accounts were compromised and about half a million rand was transferred illegally. The hacker gained access to the accounts by sending the users a spyware program as an attachment via email. The attachment, when opened, installs the spyware which logs all usernames and passwords. These usernames and passwords are then forwarded to the hacker. In response to these incidents ABSA has introduced some additional security features which will be discussed [SUND03].

8.9.1 Passwords and login



Access Account Number:

PIN:

User Number: 1

It is your responsibility to ensure the secrecy of your PIN

For more information on our security click on "About Security"

Newsflash:

New Internet Banking charges effective 1 April 2004.

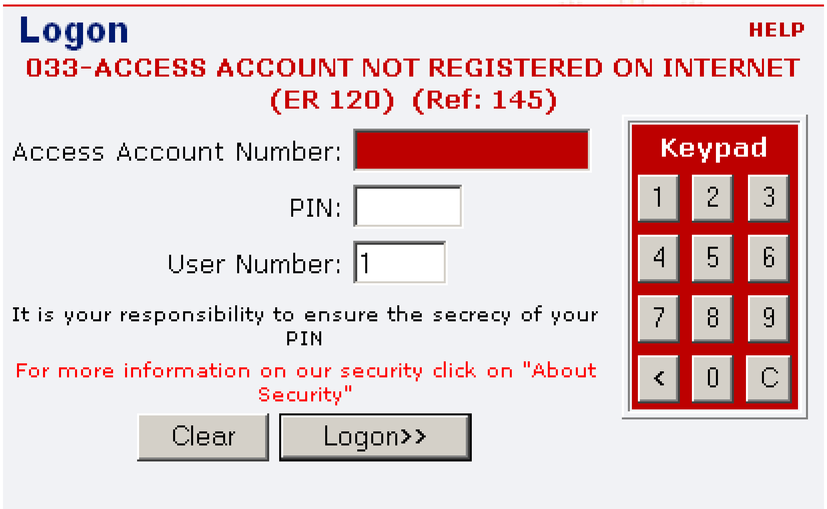
Antivirus software

* Comprehensive antivirus and personal firewall software available to Absa Internet Banking clients at no charge for one year.

Fig 8.18 ABSA login – stage 1

ABSA uses a two-stage login process. The first stage is shown in figure 8.18. The user is asked for their access account number, PIN and user number. The user number allows more than one user to have access to the same account. However, the term 'User Number' is not explained at this point. The user has the option of either typing in their details using their keyboard or using the onscreen 'keypad'. Clicking with a mouse on the keypad helps to counter spyware programs which log keys pressed. However, the keypad is not explained on the login page. The user is also not encouraged to use the keypad. This means that the security features are present but not conveyed and many users may ignore the keypad altogether because they do not know what it is there for. The user needs to follow the 'About Security' link to find out more details about the keypad and other security features. Free anti-virus software is also provided by ABSA.

Entering the incorrect account number produces the error message shown in figure 8.19. This error message is not user-friendly. Text such as '033', 'ER 120', 'Ref: 145' is included in the error message. This text will only confuse the user. A similar error message - "041-PIN INCORRECT (ER 2) (Ref: 145)" is displayed if the user enters the incorrect PIN.


Logon

033-ACCESS ACCOUNT NOT REGISTERED ON INTERNET (ER 120) (Ref: 145)

Access Account Number:

PIN:

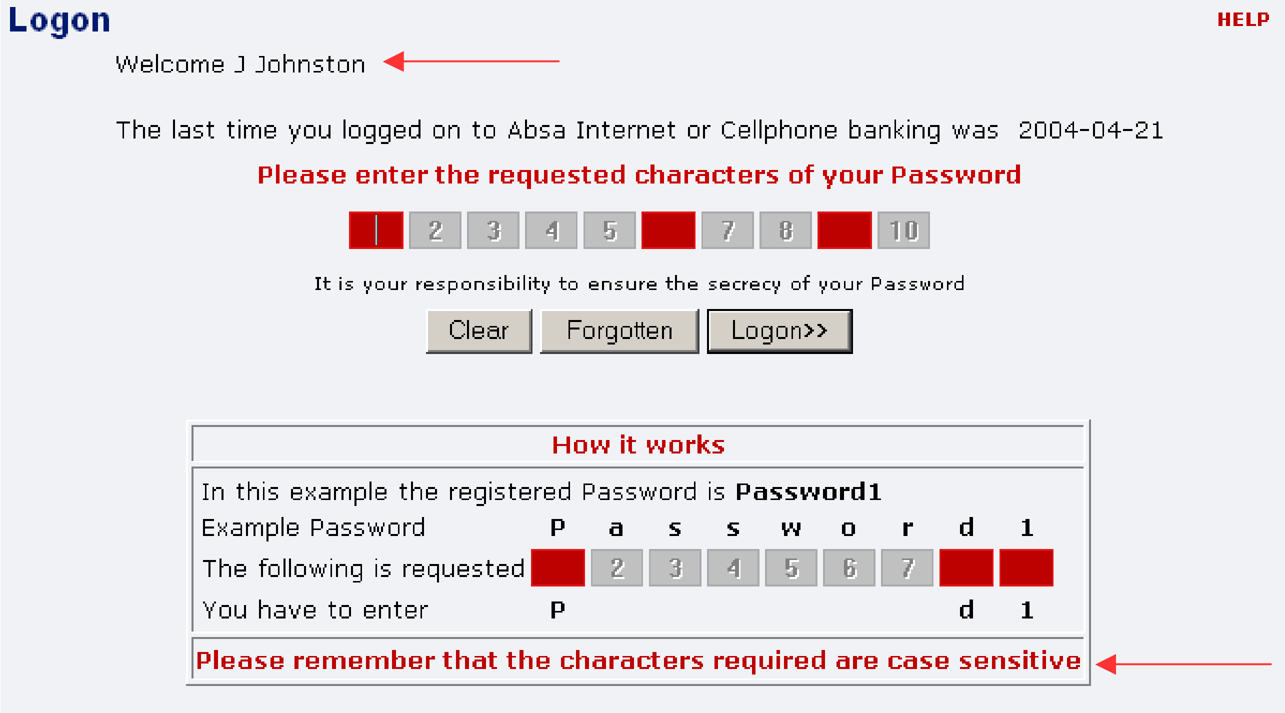
User Number: 1

It is your responsibility to ensure the secrecy of your PIN

For more information on our security click on "About Security"

Fig 8.19 Error message

Once the user has entered their account number and PIN correctly, they are welcomed by name and informed of the date of their last login. They are not informed of the time of their last login. They are then asked to enter three specific characters from their password shown in figure 8.20. This is the second stage of their login.



Logon

HELP

Welcome J Johnston

The last time you logged on to Absa Internet or Cellphone banking was 2004-04-21

Please enter the requested characters of your Password

🟥	2	3	4	5	🟥	7	8	🟥	10

It is your responsibility to ensure the secrecy of your Password

Clear | Forgotten | Logon>>

How it works

In this example the registered Password is **Password1**

Example Password	P	a	s	s	w	o	r	d	1
The following is requested	🟥	2	3	4	5	6	7	🟥	🟥
You have to enter	P							d	1

Please remember that the characters required are case sensitive

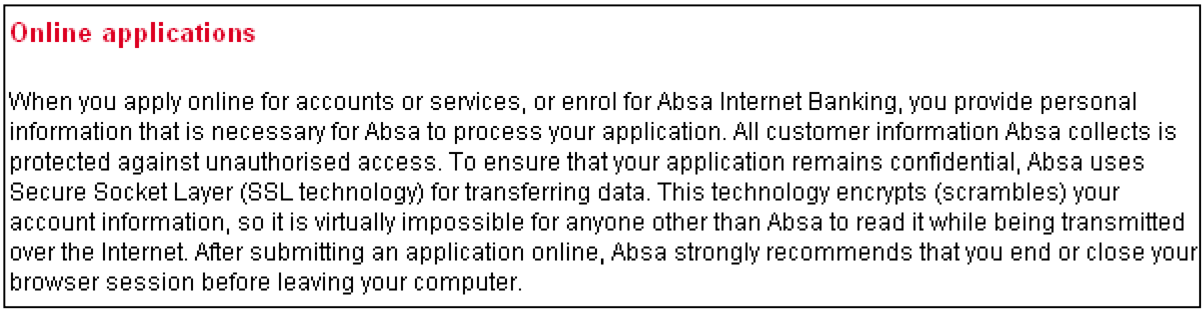
Fig 8.20 ABSA login – stage 2

Each time the user logs in, they are asked for different characters of their password. The purpose of this is to counter key logging software. A hacker would have to 'observe' a user logging in a number of times before they would have the complete password of the user.

The user is also told how this security feature works and they are encouraged to keep their password secret. A link to help is provided for additional information. This security feature enhances the security of ABSA's Internet banking. However, it hampers the usability of the site. Login takes longer and it is easy to make a mistake while trying to type in certain characters. This may cause the user to become frustrated. The user may also be tempted to write down their password to see the position of each character. The user is not reminded on this page (figure 8.20) that this added inconvenience is for their security and that it can help to protect their accounts. The user now has to remember both a PIN and a password.

8.9.2 SSL - secure connections

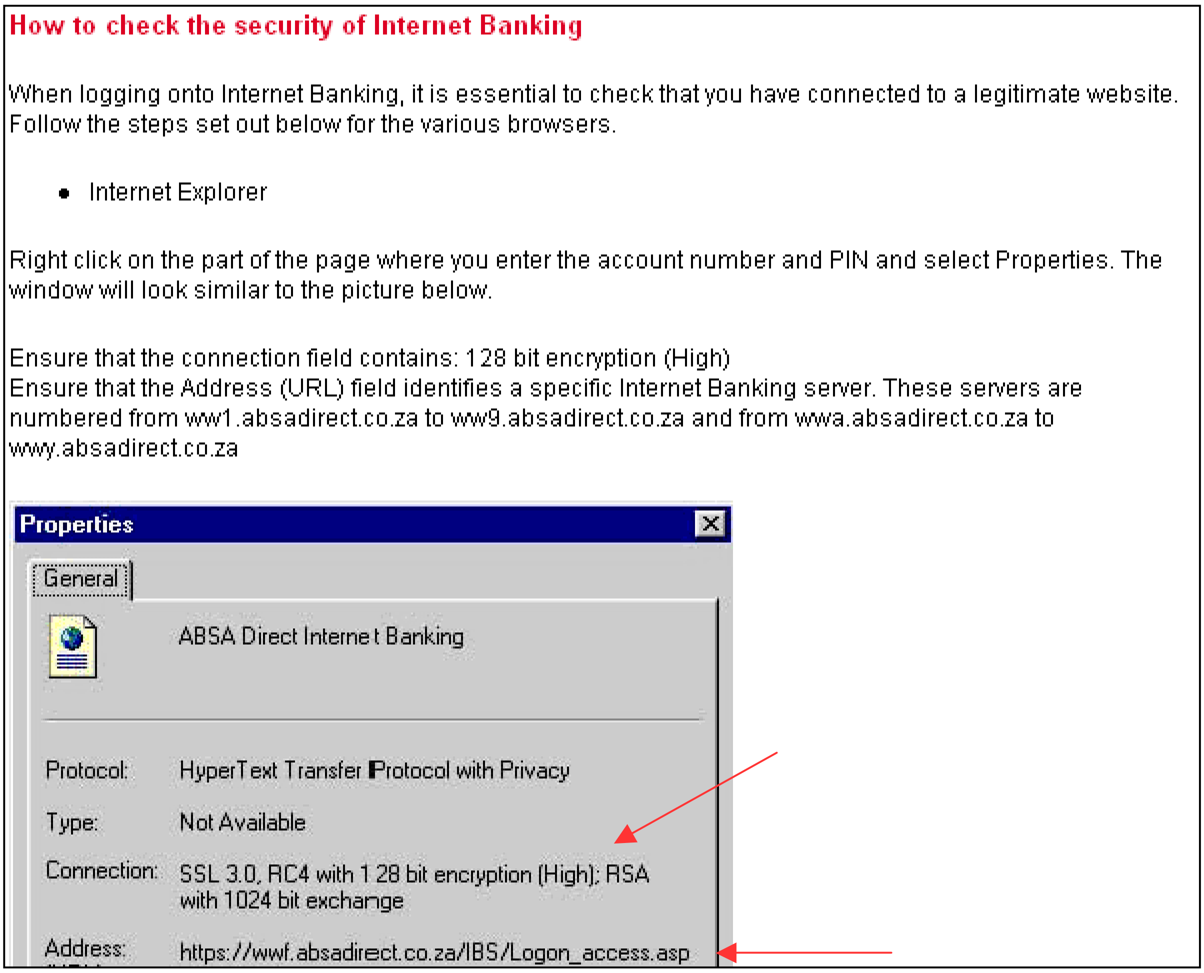
As with other banking websites ABSA uses 128-bit encryption. However, the user is not informed of this on the login page. Following the 'About Security' link provides more information on SSL (figures 8.21 and 8.22). In figure 8.22 it can be seen that the user is told how to check that their page is secure, by right clicking on it. The user's attention, however, is not drawn the padlock which is displayed by browsers when SSL is being used.



Online applications

When you apply online for accounts or services, or enrol for Absa Internet Banking, you provide personal information that is necessary for Absa to process your application. All customer information Absa collects is protected against unauthorised access. To ensure that your application remains confidential, Absa uses Secure Socket Layer (SSL technology) for transferring data. This technology encrypts (scrambles) your account information, so it is virtually impossible for anyone other than Absa to read it while being transmitted over the Internet. After submitting an application online, Absa strongly recommends that you end or close your browser session before leaving your computer.

Fig 8.21 SSL



How to check the security of Internet Banking

When logging onto Internet Banking, it is essential to check that you have connected to a legitimate website. Follow the steps set out below for the various browsers.

- Internet Explorer

Right click on the part of the page where you enter the account number and PIN and select Properties. The window will look similar to the picture below.

Ensure that the connection field contains: 128 bit encryption (High)
Ensure that the Address (URL) field identifies a specific Internet Banking server. These servers are numbered from ww1.absadirect.co.za to ww9.absadirect.co.za and from wwa.absadirect.co.za to www.absadirect.co.za

ABSA Direct Interne t Banking

Protocol: HyperText Transfer Protocol with Privacy

Type: Not Available

Connection: SSL 3.0, RC4 with 1 28 bit encryption (High); RSA with 1024 bit exchange

Address: https://wwf.absadirect.co.za/IBS/Logon_access.asp

Fig 8.22 How to check for SSL

8.9.3 Logout/logoff button

The logoff button is shown in the top right-hand corner (figure 8.23). All the banking sites analysed so far have logoff buttons in the top right-hand corner. This is advantageous to the user as they may have bank accounts with more than one bank and will be expecting the logout button to be in the same position on all banking websites.

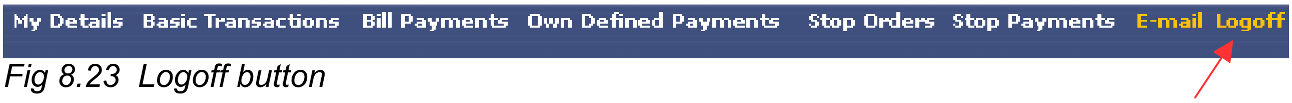
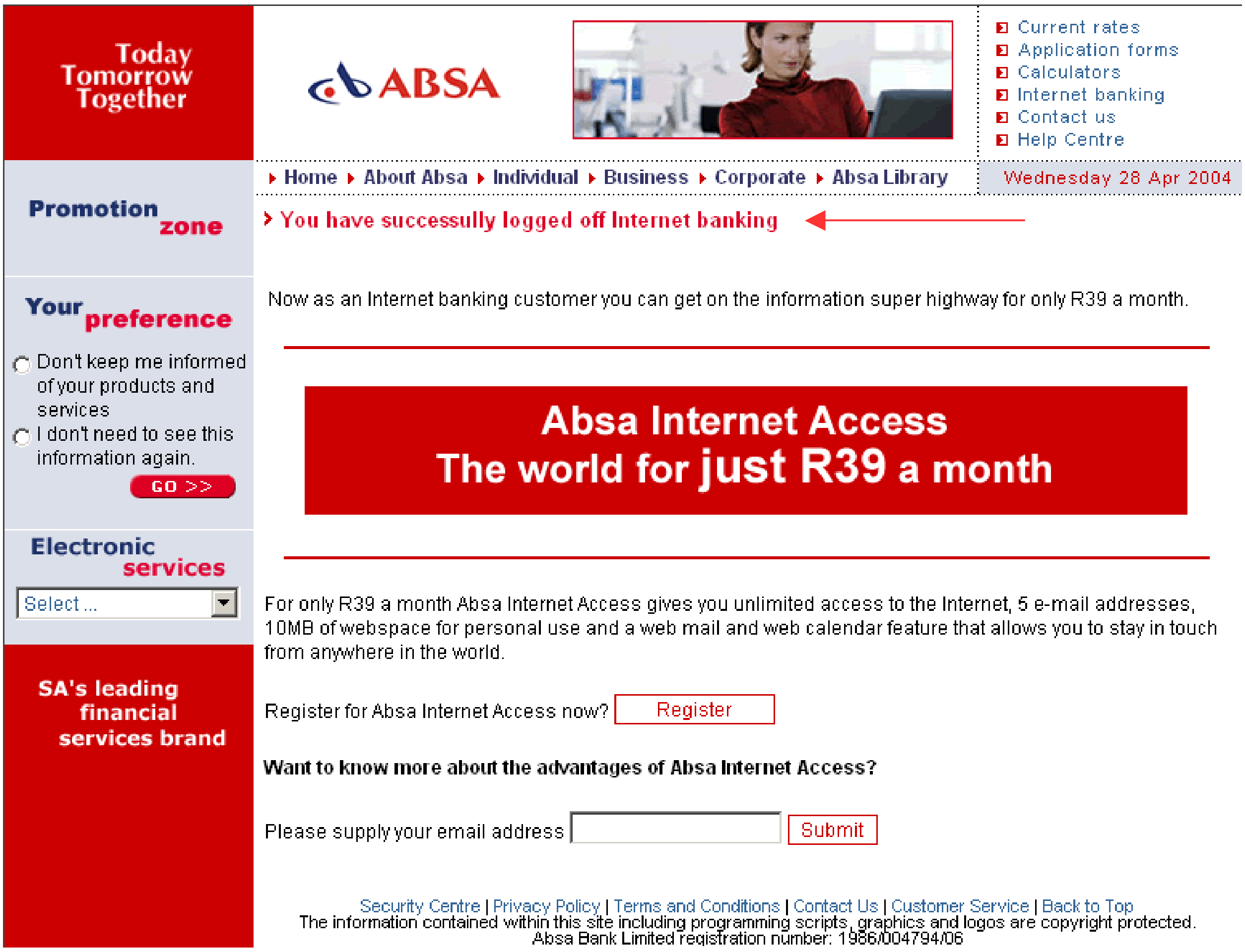


Fig 8.23 Logoff button

The logoff button, however, is small and may be overlooked. The e-mail button is also the same colour as the logoff button. This means that the user may accidentally click 'E-mail' instead of 'Logoff'. The importance of logging out is only displayed in the help. Many users may therefore never realise the importance of logging out and ending their session.

When a user logs off, the screen in figure 8.24 is shown. The screen does not have an *Aesthetic and minimalist design*. The user may miss the message informing them that the logoff was a success. The user is not informed of additional security measures that could be taken, such as emptying the temporary Internet folder, which would enhance their security.



You have successfully logged off Internet banking

○ Don't keep me informed of your products and services

○ I don't need to see this information again.

Now as an Internet banking customer you can get on the information super highway for only R39 a month.

Absa Internet Access
The world for just R39 a month

For only R39 a month Absa Internet Access gives you unlimited access to the Internet, 5 e-mail addresses, 10MB of webspace for personal use and a web mail and web calendar feature that allows you to stay in touch from anywhere in the world.

Register for Absa Internet Access now?

Want to know more about the advantages of Absa Internet Access?

Please supply your email address

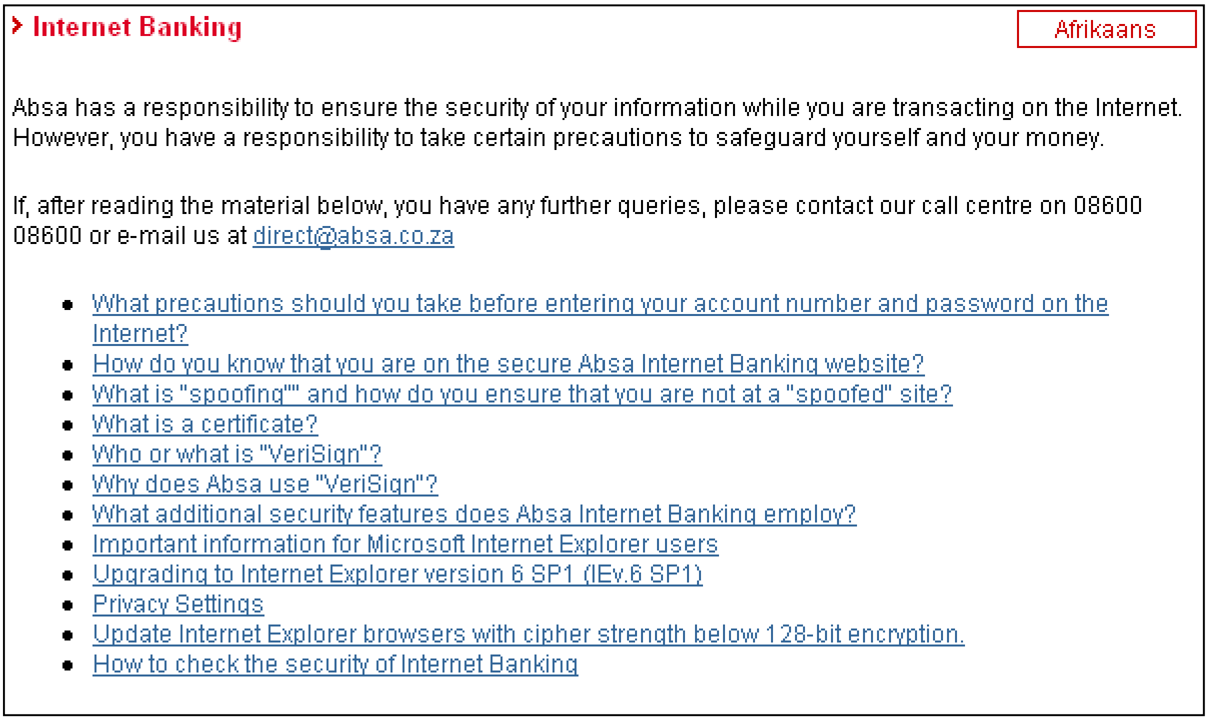
The information contained within this site including programming scripts, graphics and logos are copyright protected.
Absa Bank Limited registration number: 1986/004794/06

Fig 8.24 Logoff screen

8.9.4 Online help

ABSA provides specific help on anti-virus software, Internet banking, latest viruses and Internet banking fraud. Context-sensitive help is also provided.

Figure 8.25 shows some of the security features which are discussed. Graphics for some of the topics are given. For example pictures are given to assist the user in checking digital certificates. Topics such as phishing, firewalls and identity theft are also discussed in an easily understandable manner. One feature which is not mentioned in the help is the padlock icon displayed in the bottom right-hand corner of some browsers.



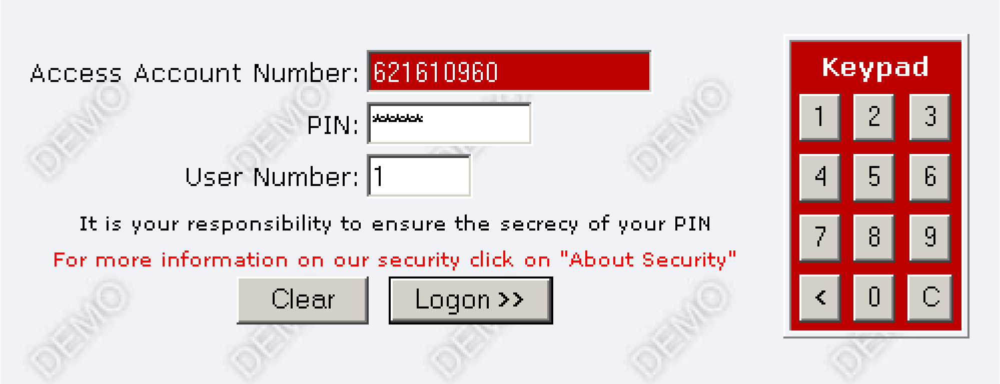
Absa has a responsibility to ensure the security of your information while you are transacting on the Internet. However, you have a responsibility to take certain precautions to safeguard yourself and your money.

If, after reading the material below, you have any further queries, please contact our call centre on 08600 08600 or e-mail us at direct@absa.co.za

- What precautions should you take before entering your account number and password on the Internet?
- How do you know that you are on the secure Absa Internet Banking website?
- What is "spoofing"" and how do you ensure that you are not at a "spoofed" site?
- What is a certificate?
- Who or what is "VeriSign"?
- Why does Absa use "VeriSign"?
- What additional security features does Absa Internet Banking employ?
- Important information for Microsoft Internet Explorer users
- Upgrading to Internet Explorer version 6 SP1 (IEv.6 SP1)
- Privacy Settings
- Update Internet Explorer browsers with cipher strength below 128-bit encryption.
- How to check the security of Internet Banking

Fig 8.25 Help

A demo option is also given for Internet banking (figure 8.26). This allows the user to login and explore the site using a default account number and password. This may assist the user in trusting the site, as they will be able to try it out before using their own personal details. However, the user is not guided through the demo and security features are not highlighted.



Access Account Number: 621610960

PIN: *****

User Number: 1

It is your responsibility to ensure the secrecy of your PIN

For more information on our security click on "About Security"

Fig 8.26 Demo login

8.10 Conclusion of ABSA.co.za analysis

8.10.1 Passwords/login

Table 8.22 summarises the analysis of the passwords/login component of ABSA.

Table 8.22 Passwords/login

Criteria	***Conclusion***	***Impact***	
Convey features (16.6% weighting)	**Partial** The keypad and user number are not explained on the login page. The reason for the extra password is also not detailed. The user needs to look in the help for additional information.	A user who has key logging software on their computer may have their account compromised because they did not use the keypad.	8.3%
Visibility of system status (16.6% weighting)	**Partial** The user is told only the date of last login.	User will not be made aware of illegal access if it occurs on the same day as a legal login.	8.3%
Learnability (16.6% weighting)	**Partial** Help explains features.	User will use the features if they read the help.	8.3%
Aesthetic and minimalist design (16.6% weighting)	**YES** Login is found on Internet banking home page.	Pages load quickly.	16.6%
Errors (16.6% weighting)	**Partial** Error messages are clear to understand, but they contain error codes.	Error codes may confuse users. The codes will, however, help to identify the error if a user contacts customer support.	8.3%

Criteria	*Conclusion*	*Impact*	
Satisfaction (16.6% weighting)	**Partial** Use of the extra password lengthens the login process. The user is not informed that the extra security features are there for their benefit.	Users may become frustrated during login. Users may also not understand why there are extra security features. The user has to remember a PIN and a password.	8.3%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 58% level of trust has been developed.	**Total**	**58%**

A 58% level of trust is fostered during the login process. ABSA offers a number of additional security features which help to make Internet banking safer for users. However, the reasons for these features are not adequately conveyed to the user.

8.10.2 SSL

The conclusion and impact for the SSL component are presented in table 8.23.

Table 8.23 SSL

Criteria	*Conclusion*	*Impact*	
Convey features (33.3% weighting)	**Partial** The purpose of SSL is conveyed to the user in the online help. No mention of it is made on the home page.	User may not be aware that their transactions are secure.	16.6%
Visibility of system status (33.3% weighting)	**Partial** The user may not be aware that SSL is being used.	The user may not use the system.	16.6%
Learnability	Not applicable.	Not applicable.	
Aesthetic and minimalist design	Not applicable.	Not applicable.	
Errors	Not applicable.	Not applicable.	

Criteria	*Conclusion*	*Impact*	
Satisfaction (33.3% weighting)	**Partial** Users who consult the help will understand that their transactions are being encrypted.		16.6%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 50% level of trust has been developed.	**Total**	**50%**

ABSA does not adequately meet any of the HCI-S criteria for SSL. The main reason for this is that the user is not told on the login page that efforts have been made to ensure that Internet banking is safe.

8.10.3 Logout button

A level of trust for the logout button component is calculated in table 8.24.

Table 8.24 Logout button

Criteria	*Conclusion*	*Impact*	
Convey features (25% weighting)	**Partial** The importance of logging out is only highlighted in the help. The user is encouraged to end their session.	A user who has not read the help may not logout.	12.5%
Visibility of system status (25% weighting)	**Yes** A message is displayed which states that the user has successfully logged out. However, the logout page is cluttered.	Logout message may be missed.	25%
Learnability	Not applicable.	Not applicable.	
Aesthetic and minimalist design (25% weighting)	**Partial** The logout button is small. However, it is yellow which may attract the user's attention to it.	User may overlook the logout button.	12.5%
Errors	An environment which generated errors could not be created.		
Satisfaction (25% weighting)	**Partial** If the user does not see the logout message, they may wonder why they had to logout in the first place.	The user may close the browser instead of logging out.	12.5%
Does the interface lead to trust being developed?			

Criteria	***Conclusion***	***Impact***	
Trust (100% weighting)	A 63% level of trust has been developed.	**Total**	**63%**

ABSA scores better with regard to the logout button. Having a dedicated logout page would help to increase this level of trust.

8.10.4 Online help

The final component – online help – is presented in table 8.25.

Table 8.25 Online help

Criteria	***Conclusion***	***Impact***	
Convey features (25% weighting)	**Yes** Features are explained in an easy-to-understand manner. Diagrams are used.	Most users will understand the help provided.	25%
Visibility of system status	Not applicable.	Not applicable.	
Learnability (25% weighting)	**Yes** Help is context-sensitive. Clear instructions are given. Additional help is given on the latest viruses.	Help is easy to use.	25%
Aesthetic and minimalist design (25% weighting)	**Yes** Navigation bar is given.	Finding the required topic should be easy.	25%
Errors	Not applicable.	Not applicable.	
Satisfaction (25% weighting)	**Yes** A user should find the help useful. Demo login should increase the user's confidence in the system.	The discussion of topics such as firewalls and phishing software will be beneficial to the user.	25%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 100% level of trust has been developed.	**Total**	**100%**

Along with eBucks, ABSA's online help adequately meets all the HCI-S criteria. The user should enjoy using the help and should be able to implement the available security features after consulting the help.

Overall ABSA scores:

58% login/passwords

50% SSL

63% logout button

100% online help

giving an average level of trust of 68%.

This means that ABSA has an average interface with regard to security (see table 5.9). Explanations and reasons for ABSA's additional security features of the keypad and extra password need to be incorporated on the first page the user visits. It should not be possible for a user to logon without being aware of the purpose and importance of these features.

Recommendations will be made in the following paragraphs.

8.11 Recommendations for ABSA.co.za

8.11.1 Recommendations for passwords/login

Recommendations are given in the following table:

Table 8.26 Passwords/login

Criteria	***Recommendation***	***Conclusion after recommendation***	***Proposed score***
Convey features	Provide an explanation on the login page for the keypad and encourage the user to use it. Reassure the user that the inconvenience of the second password is for their security.	**YES** Users are more likely to use the keypad.	16.6%
Visibility of system status	Inform the user of the date and time of last login.	**YES** User will be reassured that their account has not been tampered with.	16.6%
Learnability	Provide an explanation of the keypad on the login page.	**Partial** Users still may find the second password difficult to use.	8.3%

Criteria	*Recommendation*	*Conclusion after recommendation*	*Proposed score*
Aesthetic and minimalist design	Criterion has been met.		16.6%
Errors	Remove error codes from error messages.	**YES** Most users will be able to understand the error messages.	16.6%
Satisfaction	Reassure the user that the inconvenience of the second password is for their security.	**YES** Most users will accept the extra inconvenience if they see the benefit of increased security.	16.6%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 92% level of trust has been developed.	**Total**	**Proposed: 92%** **Existing: 58%**

By applying the HCI-S criteria the level of trust can be improved dramatically. For the component of passwords/login to score 100%, the use of the second password would need to be removed. This would increase the usability of the site, but reduce the security of the user's account. A 92% level of trust is adequate, so it is therefore recommended that the second password remain part of the login procedure.

8.11.2 Recommendations for SSL component

A trust score for the SSL component is given in the following table:

Table 8.27 SSL

Criteria	*Recommendation*	*Conclusion after recommendation*	*Proposed score*
Convey features (33.3% weighting)	Mention the use of SSL on the home page.	**YES** User will be aware that the connection is secure.	33.3%
Visibility of system status (33.3% weighting)	Draw the user's attention to the small padlock. Perhaps request certification from a third party such as VeriSign.	**YES** Users will login with confidence.	33.3%
Learnability	Not applicable.	Not applicable.	

Criteria	***Recommendation***	***Conclusion after recommendation***	***Proposed score***
Aesthetic and minimalist design	Not applicable.	Not applicable.	
Errors	Not applicable.	Not applicable.	
Satisfaction (33.3% weighting)	Users will be aware that security measures are being implemented to ensure the safety of their transactions.	**YES**	33.3%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 100% level of trust has been developed.	**Total**	**Proposed: 100%** **Existing: 50%**

The HCI-S criteria have been used to double the level of trust for the SSL component. Implementing the VeriSign seal of approval will help the interface to meet the HCI-S criteria, but it will also increase the costs of running the website. This is because a costly process needs to be followed to be verified by VeriSign.

8.11.3 Recommendations for logout button component

Recommendations for the logout button component are suggested in the following table:

Table 8.28 Logout button

Criteria	***Recommendation***	***Conclusion after recommendation***	***Proposed score***
Convey features	On each page, encourage user to logout. Highlight the importance of logging out.	**Partial** Most users will logout correctly upon ending their session.	12.5%
Visibility of system status	Criterion has been met.		25%
Learnability	Not applicable.	Not applicable.	
Aesthetic and minimalist design	Enlarge the logout button and separate it from the 'e-mail' link. Keep the logout button yellow.	**YES** Users will be able to find the logout button.	25%

Criteria	*Recommendation*	*Conclusion after recommendation*	*Proposed score*
Errors	An environment which generated errors could not be created.		
Satisfaction (25% weighting)	Thank the user for logging out and display a prominent message reassuring them that their session has now been closed. Encourage them to close the browser and empty their cache.	**YES** User will develop a habit of logging out.	25%
Does the interface lead to trust being developed?			
Trust (100% weighting)	An 88% level of trust has been developed.	**Total**	**Proposed: 88%** **Existing: 63%**

As can be seen from the above table, a number of cosmetic changes can be made which will increase the likelihood of a user logging out correctly.

8.11.4 Recommendations for the online help component

Two recommendations for the online help component are presented in the following table:

Table 8.29 Online help

Criteria	*Recommendation*	*Conclusion after recommendation*	*Proposed score*
Convey features	Criterion has been met.		25%
Visibility of system status	Not applicable.	Not applicable.	
Learnability	Criterion has been met. Perhaps include more graphics.	**YES**	25%
Aesthetic and minimalist design	Criterion has been met.		25%
Errors	Not applicable.	Not applicable.	
Satisfaction	Criterion has been met. Perhaps include an online search feature.	**YES**	25%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 100% level of trust has been developed.	**Total**	**100%**

As with eBucks.com, ABSA's existing online help component satisfies all the HCI-S criteria. Extra graphics and a search facility could be added.

The combined level of trust for all the components is presented in table 8.30. As can be seen from the table, implementing the HCI-S criteria can help the interface to foster a higher level of trust.

Table 8.30 Overall score after recommendations

	Existing	***Proposed***
Login/passwords	58%	92%
SSL	50%	100%
Logout button	63%	88%
Online help	100%	100%
Average	**68%**	**95%**

In the next section the reasons behind the different levels of trust will be discussed.

8.12 Reasons why certain banking sites foster a higher level of trust

Table 8.31 shows the comparison between the three banks. It can be seen that eBucks has the highest level of trust, followed by ABSA and then Nedbank. eBucks also has the highest score for three of the four components.

Table 8.31 Comparison of Nedbank, eBucks and ABSA

	Nedbank	***eBucks***	***ABSA***
Login/passwords	58%	**83%**	58%
SSL	50%	**83%**	50%
Logout button	**75%**	40%	63%
Online help	75%	**100%**	**100%**
Average level of trust	65%	**77%**	68%

8.12.1 Login/passwords

After analysing the three banking websites, it was found that the login/passwords component can be made up of four elements shown in table 8.32. The reason why eBucks has obtained the highest level of trust is that it implements three of the four elements correctly. Implementing these elements leads to adequate fulfilment of the HCI-S criteria, which in turn generates a high level of trust.

Table 8.32 Login/passwords comparison

	Nedbank	***eBucks***	***ABSA***
User is greeted by name	No	Yes	Yes
User is told of date and time of last login	No	Yes	(User is only told of date)
User-friendly error messages	No	Yes	No
User reminded to keep login details a secret	No	No	Yes

Nedbank has not implemented any of these elements during login and has therefore scored poorly. ABSA has implemented only two and also scores poorly.

8.12.2 SSL

Table 8.33 presents a comparison between the three banking websites with regard to the SSL component.

Table 8.33 SSL

	Nedbank	***eBucks***	***ABSA***
Inform the user on the home page that they are accessing a secure site	Yes	Yes	No
Draw the user's attention to the padlock	No	No	No
Use third-party logos for endorsement, e.g. VeriSign	No	Yes	No

Both Nedbank and ABSA score poorly in this component. eBucks implements two of the three elements and has the highest level of trust.

8.12.3 Logout button

A comparison between the elements found on the logout button component is shown in table 8.34.

Table 8.34 Logout button

	Nedbank	**eBucks**	**ABSA**
Prominent position (top right)	Yes	Yes	Yes
Large	Yes	No	No
Dedicated logout page informing user of the success of the logout	Yes	Yes	Yes
Encourage user to empty cache and close browser on logout page	No	(Encouraged to close browser)	No
Explain importance of logging out in help	Yes	Yes	Yes
Encourage users to logout on each page	No	No	No

Nedbank's logout button component implements the most elements. As expected, Nedbank also fosters the highest level of trust with this component compared to eBucks and ABSA.

8.12.4 Online help

Table 8.35 illustrates the elements which make up the online help component.

Table 8.35 Online help

	Nedbank	**eBucks**	**ABSA**
Context-sensitive help	Yes	Yes	Yes
Use of images and graphics to explain security features	No	Yes	Yes
Explain concepts in simple terms	Yes	Yes	Yes
User-friendly navigation	No	Yes	Yes
Provide additional help on topics such as viruses, firewalls, spyware and phishing	Yes	Yes	Yes

All three banks scored highly in the online help component. Both eBucks and ABSA meet all the HCI-S criteria. This is evident from table 8.35 which shows that all the elements are implemented for these two banks.

The above elements for each component can be used along with the HCI-S criteria to design online banking interfaces which are easy to use and secure.

8.13 Conclusion

In this chapter the Internet banking websites of Nedbank, FNB and ABSA were analysed according to the HCI-S criteria. Various components of each site were examined and the level of trust fostered for each site calculated. This means that the first two objectives of the chapter have been satisfied. The third objective of this chapter has also been met by identifying various elements which, when implemented, would help to foster high levels of trust. The aim of this chapter, i.e. to calculate the level of trust for each site, has therefore been met.

Recommendations on how the interfaces of each site can be improved were also made. These recommendations are generally cost-effective and easy to implement. Making minor modifications to an interface can normally be accomplished in a short time frame. Implementing these recommendations will help to ensure that users are familiar with the security features available and will implement them correctly. Conducting transactions on the Internet can be nerve-racking; applying the HCI-S criteria will help to build trust between the user and the banking site. The higher the level of trust, the more the user will be willing to use the service and the more they will enjoy using it.

In the next chapter three e-commerce interfaces will be examined.

Chapter 9
Evaluation of E-commerce Websites

9.1 Introduction

Security forms the cornerstone of electronic commerce. Without a safe, secure shopping environment, it is impossible for e-commerce to become mainstream. Security needs to be a priority right from the planning stages of an e-commerce site. Graphics, visualisation and usability surveys have shown that security is the biggest concern among online consumers [TIWA99]. The interface of a website plays a crucial role when it comes to security. This is because the user experiences the security features through the interface. If these security features are not explained by the interface or the interface does not guide the user, then the user will not trust the website and may leave.

One of the barriers to online shopping is the websites' interface or 'storefront'. 40% of the users surveyed in a PriceWaterhouseCoopers study stated that being unfamiliar with the electronic storefront was a barrier to their online shopping [BERN01]. In another study 33% of the people surveyed indicated having difficulty locating products and 62% even left a website because they could not find what they wanted to buy [BERN01]. E-commerce websites need to strike a balance between usability and security.

Business-to-customer e-commerce continues to grow. It is expected that by the end of 2004 over $300 billion will have been spent online by consumers [BERN01]. In South Africa R24 billion is expected to be spent online in 2005 [BIM00]. From these figures it is obvious that companies are constantly looking for ways to attract more online customers and also, importantly, for ways on how to keep existing customers.

In chapter 7, e-commerce sites were divided into three broad categories – e-tailers, services and electronic banking. Three websites found in the electronic banking category were examined in chapter 8. This chapter will concentrate on the two remaining categories of services and e-tailers.

The most commonly purchased items online by South Africans are groceries, books, music and entertainment products [ONLI02]. For this chapter the following three websites, which sell the above products, have therefore been chosen:

- Picknpay.co.za, an e-tailer which sells groceries,
- Kalahari.net, an e-tailer which sells books and music and

- Sterkinekor.co.za, a services company which sells entertainment products.

The aim and objectives of this chapter are similar to those of chapter 8. Chapter 8 focused on the security interface of banking sites; this chapter focuses on the security interfaces of e-tailers and online services sites. The aim of the chapter is to use the HCI-S criteria to calculate the level of trust fostered by each interface. In order to accomplish this aim, each interface first needs to be analysed according to the HCI-S criteria. The second objective is then to attempt to quantify the level of trust fostered by each interface based on the analysis. The last objective is to try to pinpoint the reasons why some interfaces foster a higher level of trust than others.

This chapter is lengthy due to the large number of screen grabs and tables. It has therefore been divided into three sections:

- Section A – Analysis and recommendations for Sterkinekor.co.za
- Section B – Analysis and recommendations for Kalahari.net
- Section C – Analysis and recommendations for Picknpay.co.za

9.2 Components used

In chapter 7, HCI and E-commerce, it was seen that the security interface of a website is made up of various components. Table 9.1 shows the components used by Sterkinekor.co.za, Kalahari.net and Picknpay.co.za.

Table 9.1 Components used

	Registration	***Passwords/ login***	***SSL***	***Shopping cart & checkout***	***Logout button***	***Online help***
E-tailers						
Kalahari.net	**X**	**X**	**X**	**X**		**X**
Picknpay.co.za	**X**	**X**	**X**	**X**	**X**	**X**
Services						
Sterkinekor.co.za			**X**			**X**

Picknpay.co.za uses all of the components, Kalahari.net does not use a logout button and Sterkinekor.co.za currently implements only two of the components – SSL and online help. During the course of this dissertation Sterkinekor implemented some major changes to their website. Table 9.2 highlights the differences between the website available during

2003 (v2003 of Sterkinekor.co.za) and the website available during 2004 (v2004 of Sterkinekor.co.za).

Table 9.2 Sterkinekor 2003 site vs. 2004 site

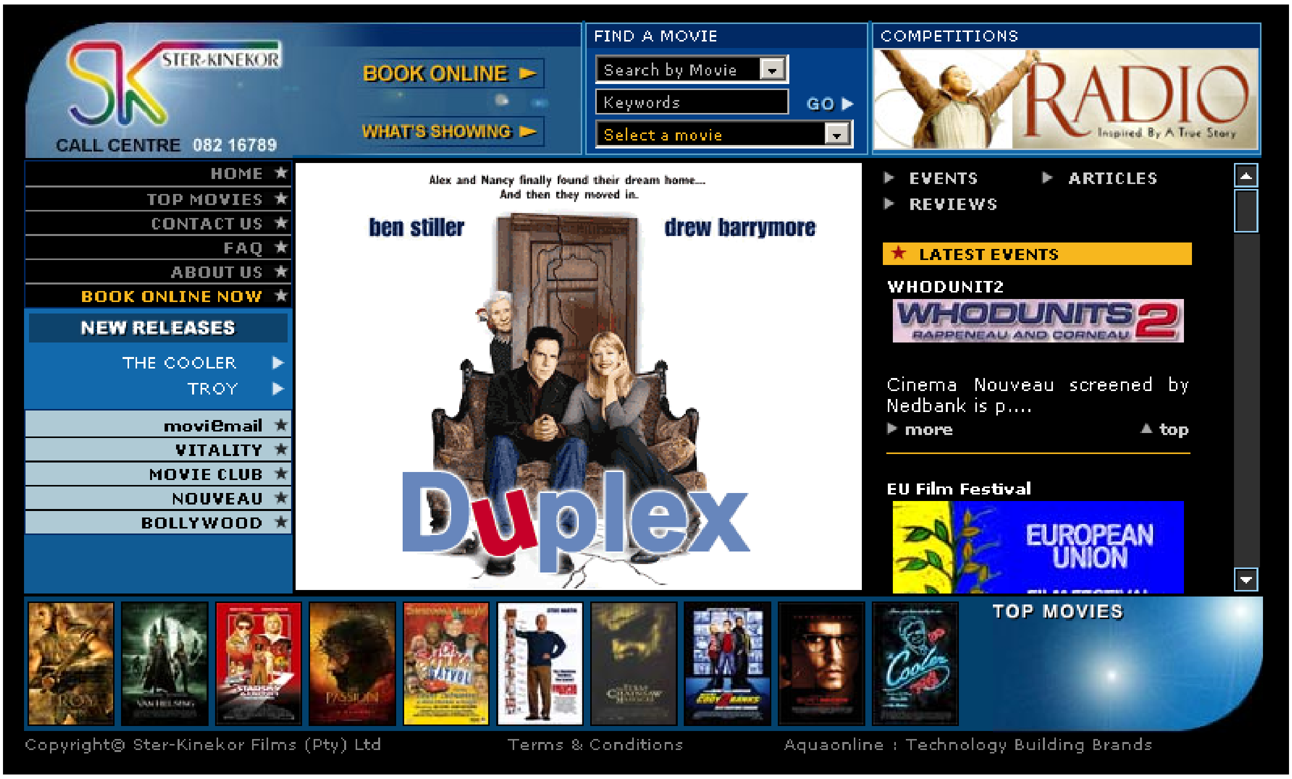
	Registration	***Passwords/ login***	***SSL***	***Shopping cart & checkout***	***Logout button***	***Online help***
v 2003	X	X	X			X
v 2004			X			X

Some of the changes made have improved the interface, while other modifications have led to the security of the site being lowered. Aspects of both interfaces are highlighted as necessary.

SECTION A

9.3 Analysis of Sterkinekor.co.za

Sterkinekor is one of the two largest movie houses in South Africa. Being an entertainment company Sterkinekor has opted for a graphically rich website. The home page is shown in figure 9.1. As can be seen, it is attractive and pleasing to the eye. Sterkinekor.co.za is professionally designed and creates a positive image for the movie house. However, it does not have a *minimalist* design and the page takes a long time to download over a 56K dial-up connection.



Cinema Nouveau screened by Nedbank is p....

Copyright© Ster-Kinekor Films (Pty) Ltd Terms & Conditions Aquaonline : Technology Building Brands

Fig 9.1 Sterkinekor.co.za home page

9.3.1 Registration

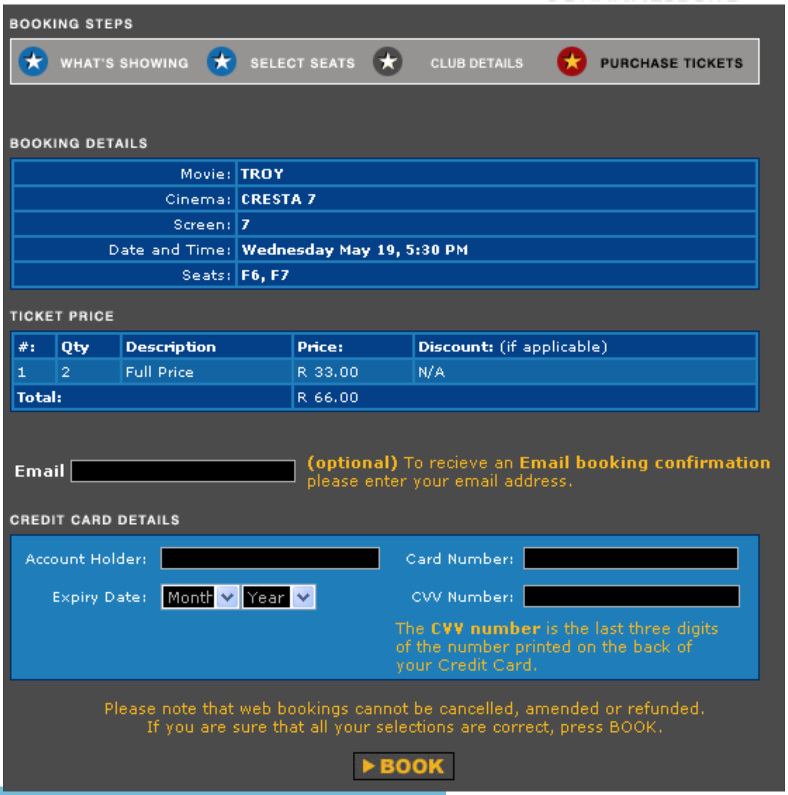
Sterkinekor.co.za originally implemented compulsory registration (v2003). A user had to register before purchasing tickets. The enforced registration was inconvenient and had a negative impact on the usability of the site. In v2004 of Sterkinekor.co.za the registration has been removed. This is a positive decision as it is now much quicker to purchase a ticket. The user also has one less username and password to remember.

9.3.2 Passwords/login

As expected, removing the registration component means that the passwords/login component is no longer available in v2004 of Sterkinekor.co.za. Removing the passwords/login component may lead to the level of trust diminishing. This is because the process of logging in helps to foster trust. The user enters their own private password and is logged in. This helps to create an environment in which the user feels secure. Once logged in, a user will feel that they are not entering their credit card details on a 'public' page. They have had to login to a 'secure' page. For many users, using a password equates to security. From a technical perspective logging in does not make the credit card details any more or any less secure, as long as both pages use SSL.

9.3.3 SSL – secure connections

Sterkinekor.co.za uses SSL technology to secure the connection. However, the user is not at any stage informed of any security features while filling in their credit card details (figure 9.2). There is no mention of encryption, SSL, or anything else which would assure the user that their credit card number will be safe. The *Visibility of system status* is not clear, which leads to a lack of *Trust*. Limited information on security is available in the online help.



BOOKING STEPS

BOOKING DETAILS

Movie:	TROY
Cinema:	CRESTA 7
Screen:	7
Date and Time:	Wednesday May 19, 5:30 PM
Seats:	F6, F7

TICKET PRICE

#:	Qty	Description	Price:	Discount: (if applicable)
1	2	Full Price	R 33.00	N/A
Total:			R 66.00	

Email

(optional) To recieve an **Email booking confirmation** please enter your email address.

CREDIT CARD DETAILS

Account Holder:

Card Number:

Expiry Date: Month Year

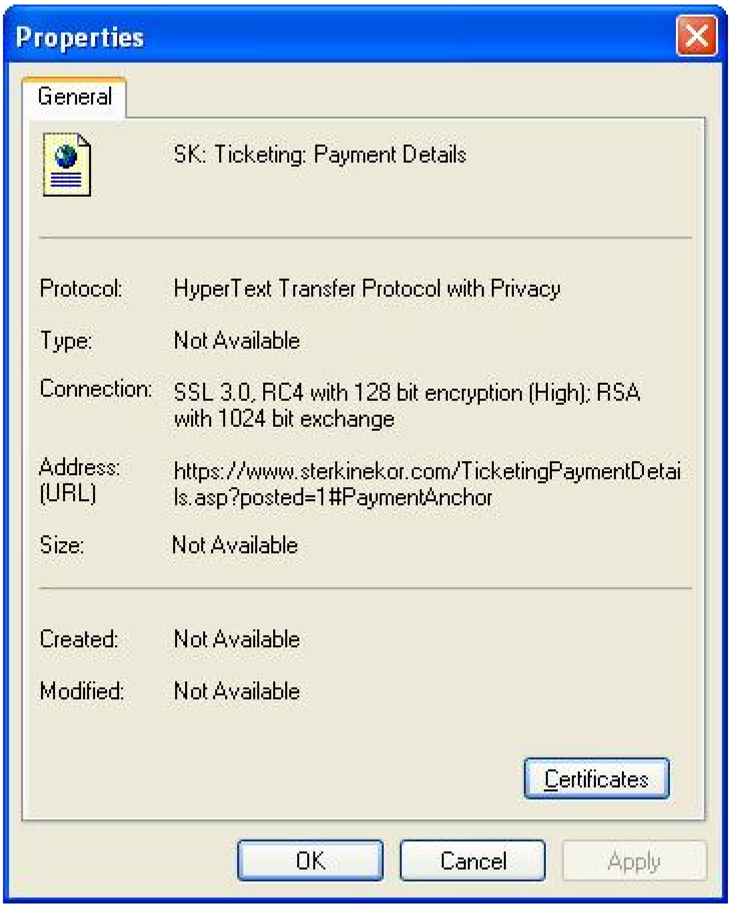
CVV Number:

The **CVV number** is the last three digits of the number printed on the back of your Credit Card.

Please note that web bookings cannot be cancelled, amended or refunded.
If you are sure that all your selections are correct, press BOOK.

Fig 9.2 Credit card information

Sterkinekor.co.za uses 128-bit encryption on the credit card page (figure 9.2). However, with some browsers a padlock is not shown in the bottom right-hand corner of the browser's window. In addition, some versions of Internet Explorer display 'http' instead of 'https' in the URL. In order to confirm that the page is indeed being encrypted, the user needs to right click on the page and select 'Properties'. The window shown in figure 9.3 is now displayed. Under the 'Connection' heading it can be seen that encryption is being used and the 'Address' (URL) heading shows that the page being viewed is an 'https' page.



SK: Ticketing: Payment Details

Protocol: HyperText Transfer Protocol with Privacy

Type: Not Available

Connection: SSL 3.0, RC4 with 128 bit encryption (High); RSA with 1024 bit exchange

Address: (URL) https://www.sterkinekor.com/TicketingPaymentDetails.asp?posted=1#PaymentAnchor

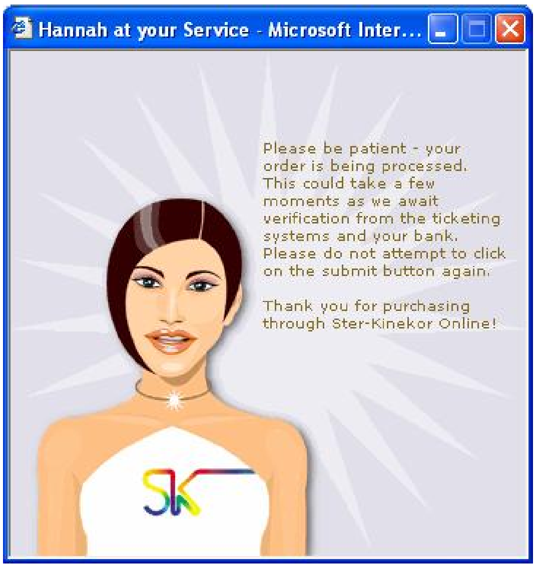
Size: Not Available

Created: Not Available

Modified: Not Available

Fig 9.3 Properties window of credit card page

Sterkinekor provides feedback to the user while the credit card transaction is being verified (figure 9.4). This aids the *Visibility of system status* and will encourage the user to *Trust* the system. A confirmation email is also sent to the user once the booking has been completed.



Hannah at your Service - Microsoft Inter...

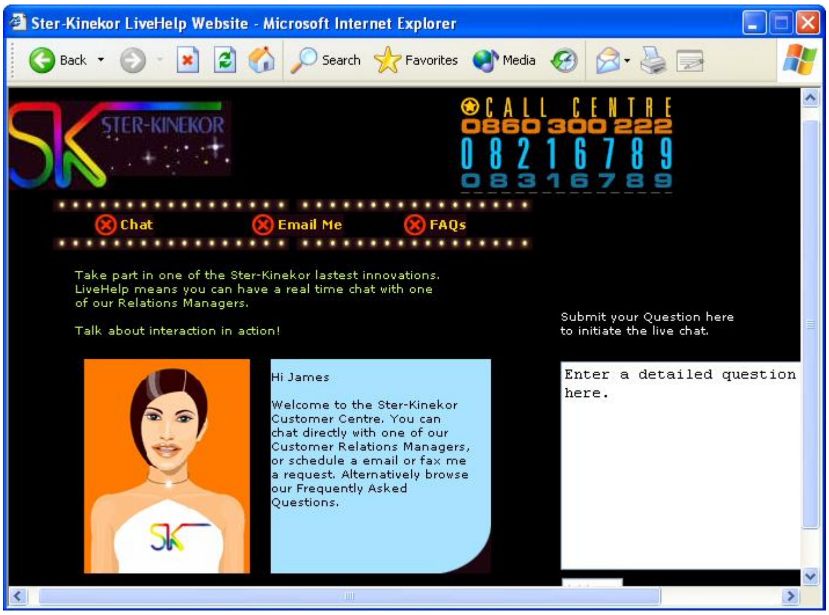
Please be patient - your order is being processed. This could take a few moments as we await verification from the ticketing systems and your bank. Please do not attempt to click on the submit button again.

Thank you for purchasing through Ster-Kinekor Online!

Fig 9.4 v2003 Payment being processed

9.3.4 Online help

The online help on Sterkinekor.co.za v2003 was comprehensive (figure 9.5). The user was able to obtain help via a live chat facility, during office hours, with a relations manager. This brought in human contact which would have helped the user in *trusting* the system, especially when sending credit card information over the Internet. The help found in v2003 provided information on Sterkinekor's privacy policy, digital certificates, SSL and encryption. The customer was offered the following guarantee: "... *is the fact that we guarantee your credit card security. You pay nothing if unauthorised charges are made to your card as a result of shopping at sterkinekor.com or of digitalmall.com's alliance partners.*"



Ster-Kinekor LiveHelp Website - Microsoft Internet Explorer

CALL CENTRE
0860 300 222
0 8 2 1 6 7 8 9
0 8 3 1 6 7 8 9

Chat Email Me FAQs

Take part in one of the Ster-Kinekor lastest innovations. LiveHelp means you can have a real time chat with one of our Relations Managers.

Talk about interaction in action!

Hi James

Welcome to the Ster-Kinekor Customer Centre. You can chat directly with one of our Customer Relations Managers, or schedule a email or fax me a request. Alternatively browse our Frequently Asked Questions.

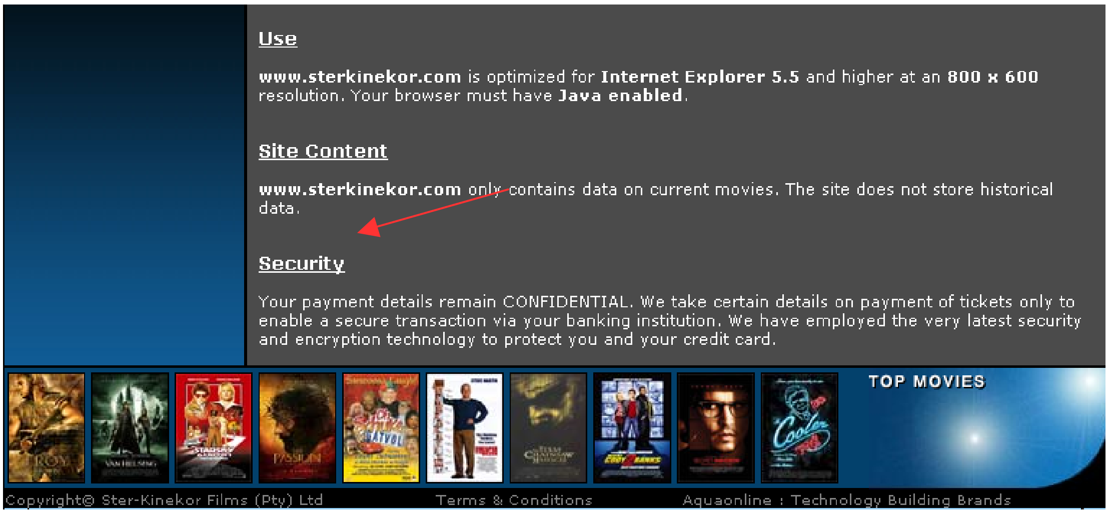
Submit your Question here to initiate the live chat.

Enter a detailed question here.

Fig 9.5 v2003 Online help

v2004 of Sterkinekor.co.za has, however, removed most of the above help features. The online chat is no longer available, information on digital certificates, SSL and encryption, and the guarantee have been removed. The content of the online help has been greatly reduced (figure 9.6 and figure 9.7). The absence of these features means that the level of *Trust* fostered has been greatly reduced. A privacy policy is still included and the user is assured that Sterkinekor has: "*... employed the very latest security and encryption technology to protect you and your credit card*".

The contents of the help file have been divided between two pages. Part of the help is found on the FAQ page. This is intuitive and most users would look under FAQ for assistance. However, the privacy and security policies are found under the 'About us' link. This is not where a user would expect to find this information. A user may therefore never see these policies, which, if read, by the user would help to foster trust.



Use

www.sterkinekor.com is optimized for **Internet Explorer 5.5** and higher at an **800 x 600** resolution. Your browser must have **Java enabled**.

Site Content

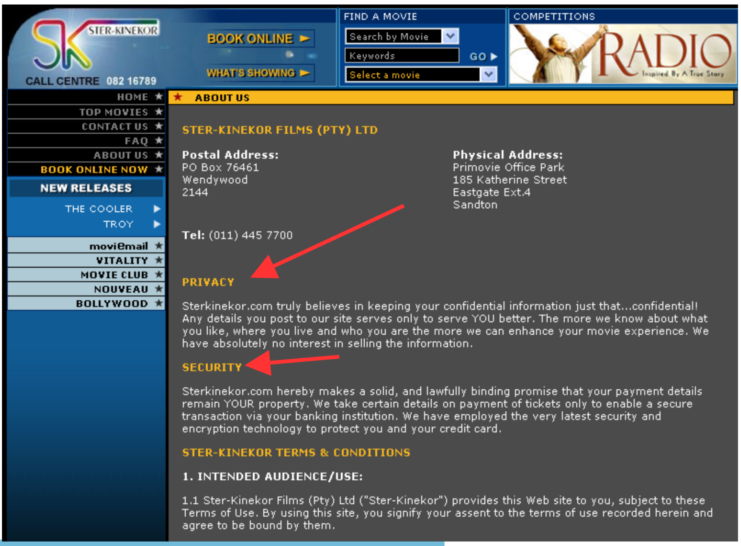
www.sterkinekor.com only contains data on current movies. The site does not store historical data.

Security

Your payment details remain CONFIDENTIAL. We take certain details on payment of tickets only to enable a secure transaction via your banking institution. We have employed the very latest security and encryption technology to protect you and your credit card.

TOP MOVIES
Copyright© Ster-Kinekor Films (Pty) Ltd
Terms & Conditions
Aquaonline : Technology Building Brands

Fig 9.6 Online help



STER-KINEKOR FILMS (PTY) LTD

Postal Address:
PO Box 76461
Wendywood
2144

Physical Address:
Primovie Office Park
185 Katherine Street
Eastgate Ext.4
Sandton

Tel: (011) 445 7700

PRIVACY

Sterkinekor.com truly believes in keeping your confidential information just that...confidential! Any details you post to our site serves only to serve YOU better. The more we know about what you like, where you live and who you are the more we can enhance your movie experience. We have absolutely no interest in selling the information.

SECURITY

Sterkinekor.com hereby makes a solid, and lawfully binding promise that your payment details remain YOUR property. We take certain details on payment of tickets only to enable a secure transaction via your banking institution. We have employed the very latest security and encryption technology to protect you and your credit card.

STER-KINEKOR TERMS & CONDITIONS

1. INTENDED AUDIENCE/USE:

1.1 Ster-Kinekor Films (Pty) Ltd ("Ster-Kinekor") provides this Web site to you, subject to these Terms of Use. By using this site, you signify your assent to the terms of use recorded herein and agree to be bound by them.

Fig 9.7 About us – security and privacy policies

9.4 Conclusion of Sterkinekor.co.za analysis

Two tables are given in this section to summarise the Sterkinekor.co.za analysis: one table for SSL and the other for online help. The same methodology used in chapter 8 to analyse the banking sites is used in this section. Table 9.3 provides an explanation of the colours used.

Table 9.3 Key

Colour	***Explanation***	***Influence on weighting***
Red	Criterion has not been met.	0% of weighting
Green	Criterion has been met.	100% of weighting
Orange	In some instances the criterion has been met, in other instances it has not.	50% of weighting
Gray	Criterion is not applicable for this component.	

9.4.1 SSL

A summary of the SSL component is given in the following table:

Table 9.4 SSL component

Criteria	***Conclusion***	***Impact***	
Convey features (33.3% weighting)	**Partial** The user is not informed on the credit card page that the connection is secure. Encryption is briefly mentioned in the online help.	User may not be aware that SSL is being used.	16.6%

Criteria	***Conclusion***	***Impact***	
Visibility of system status (33.3% weighting)	**Partial** Status of SSL is conveyed by the small padlock in Internet Explorer (IE). However, the padlock may not be shown on some versions of IE.	The user may not use the system.	16.6%
Learnability	Not applicable.	Not applicable.	
Aesthetic and minimalist design	Not applicable.	Not applicable.	
Errors	Not applicable.	Not applicable.	
Satisfaction (33.3% weighting)	**Partial** The user will probably not be aware that SSL is being used to ensure safe transactions.	The user will trust Sterkinekor.co.za because of their real-world status, not because of their website.	16.6%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 50% level of trust has been developed.	**Total**	**50%**

Sterkinekor.co.za has made a minimal effort to reassure the user that the transaction is secure. The only indication of the use of SSL is the padlock and 'https' in the URL provided by the browser.

9.4.2 Online help

A level of trust for the online help component is presented in the following table:

Table 9.5 Online help

Criteria	***Conclusion***	***Impact***	
Convey features (25% weighting)	**No** Features are not conveyed. Encryption and security are mentioned briefly. Users are given general assurances.	Users will have to visit other websites for explanations of encryption, SSL and digital certificates.	0%
Visibility of system status	Not applicable.	Not applicable.	

Criteria	*Conclusion*	*Impact*	
Learnability (25% weighting)	**No** Help is not context-sensitive. Parts of help are found under two sections – FAQ and About us.	User might never click on the 'About us' link.	0%
Aesthetic and minimalist design (25% weighting)	**Partial** Help has a minimalist design. A navigation bar is not provided.	User may find the help frustrating to use.	12.5%
Errors	Not applicable.	Not applicable.	
Satisfaction (25% weighting)	**No** Help is completely inadequate.	User will not find enough information.	0%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 12.5% level of trust has been developed.	**Total**	**12.5%**

The online help provided in v2004 is completely inadequate and this is reflected in the low score. Security features are not highlighted and explained. v2003 had a more extensive and user-friendly help which would have fostered a much higher level of trust.

Overall Sterkinekor.co.za scores:

50%	SSL
12.5%	online help

giving an average level of trust of 31%.

This means that Sterkinekor.co.za has met less than half of the HCI-S criteria. As can be seen from table 9.6 this score denotes an inadequate interface which users avoid. Despite this low score users continue to use Sterkinekor.co.za. Some possible reasons for this are that the purchase amounts for tickets are low and therefore users may be less concerned about the security of the transaction. Another reason why users continue to purchase tickets online is that Sterkinekor already has a very strong offline brand which consumers trust. As was seen in chapter 7, a strong brand can help to foster trust online. Without this strong brand, many users would not use the site.

Table 9.6 Description of scores

Overall score	*Description*	*Impact*
0%-49%	Inadequate interface	The user will avoid using the interface, which will lead to weak security.

Overall score	*Description*	*Impact*
50%-59%	Below average interface	The interface will confuse and frustrate the user.
60%-69%	Average interface	The user will tolerate the interface if they really need to use the program. They will become familiar with the interface over time.
70%-85%	Above average interface	Most of the interface will be easy to use. One or two aspects of the interface may irritate the user.
85%-100%	Excellent interface	The user will enjoy using the interface. The implementation of security features by the user is easy and intuitive.

v2004 of the site is overall an improvement on v2003. However, it would have been a prudent decision to include the help of v2003 in v2004.

9.5 Recommendations for Sterkinekor.co.za

Recommendations according to the HCI-S criteria are now given for each component of Sterkinekor.co.za.

9.5.1 Recommendations for SSL component

In table 9.7 recommendations are given for the SSL component, along with a recalculated 'proposed score'.

Table 9.7 SSL

Criteria	*Recommendation*	*Conclusion after recommendation*	*Proposed score*
Convey features (33.3% weighting)	Mention the use of SSL on the credit card page. Inform the user that measures are being taken to protect the transaction.	**YES** User will be aware that the connection is secure.	33.3%
Visibility of system status (33.3% weighting)	Draw the user's attention to the small padlock. Perhaps request certification from a third party such as VeriSign.	**YES** Users will login with confidence.	33.3%

Criteria	*Recommendation*	*Conclusion after recommendation*	*Proposed score*
Learnability	Not applicable.	Not applicable.	
Aesthetic and minimalist design	Not applicable.	Not applicable.	
Errors	Not applicable.	Not applicable.	
Satisfaction (33.3% weighting)	Users will be aware that security measures are being implemented to ensure the safety of their transaction.	**YES**	33.3%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 100% level of trust has been developed.	**Total**	**Proposed: 100%** **Existing: 50%**

Any mention of SSL will help to improve the level of trust. This could be on the home page or on the actual credit card page.

9.5.2 Online help

With regard to Sterkinekor.co.za's online help, the strongest recommendation would be to implement v2003's help component.

Table 9.8 Online help

Criteria	*Recommendation*	*Conclusion after recommendation*	*Proposed score*
Convey features	Provide explanations for SSL, encryption and digital certificates.	The user will have a better understanding of security concepts.	25%
Visibility of system status	Not applicable.	Not applicable.	
Learnability	Have one help section.	Information on security will be easier to find.	25%
Aesthetic and minimalist design	Provide a navigation bar.	Navigation of help will be easy.	25%
Errors	Not applicable.	Not applicable.	
Satisfaction	Perhaps include context-sensitive help.	Most relevant help will be displayed.	25%

Criteria	***Recommendation***	***Conclusion after recommendation***	***Proposed score***
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 100% level of trust has been developed.	**Total**	**Proposed: 100%** **Existing: 12.5%**

A number of extensive changes are necessary to improve the level of trust generated by the help component. These changes, which were present in earlier versions of the site, will lead to a substantial increase in the level of trust. The SSL component can be improved by a number of minor changes.

Table 9.9 Overall score after recommendation

	Existing	***Proposed***
SSL	50%	100%
Online help	12.5%	100%
Average	**31%**	**100%**

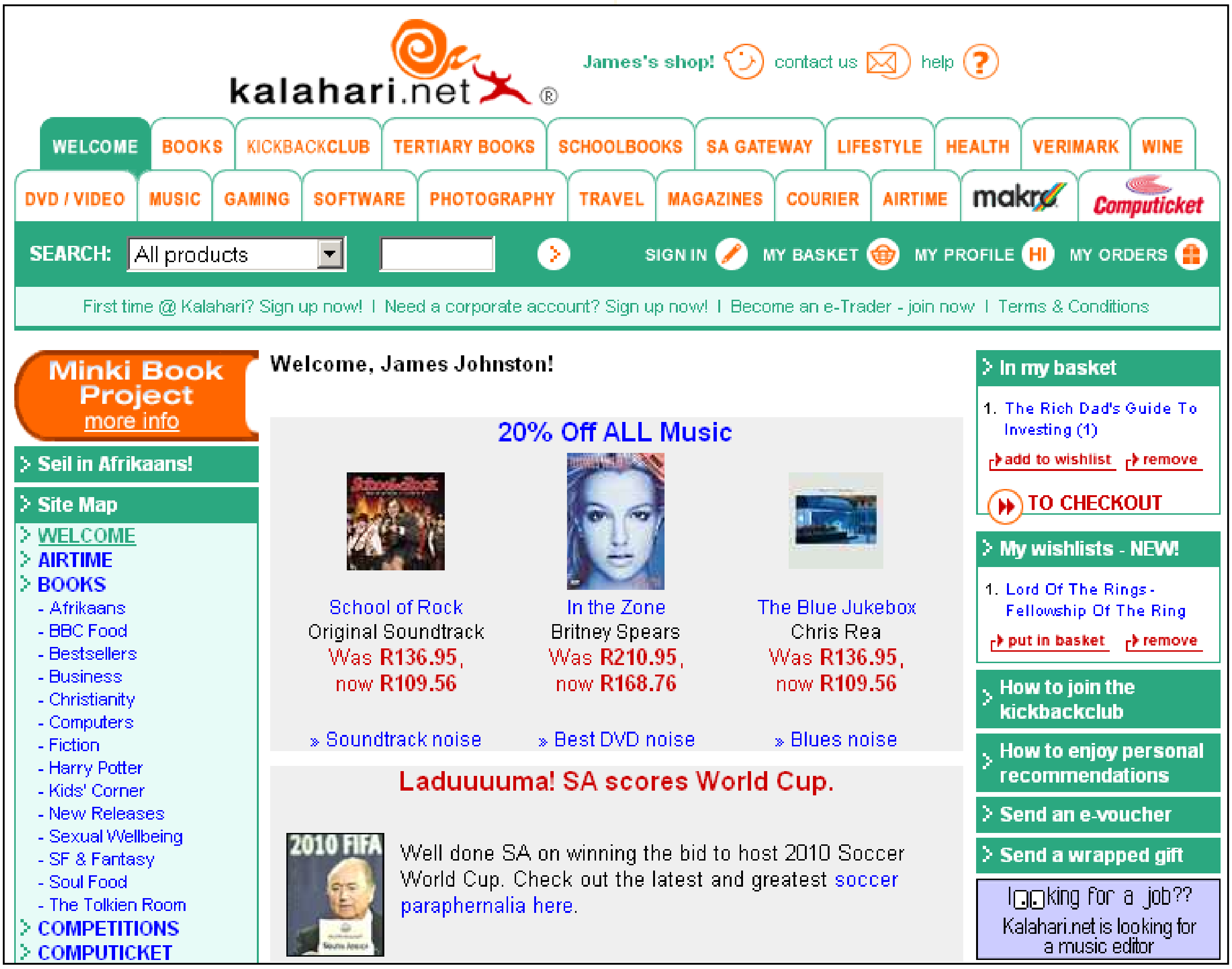
Kalahari.net is analysed in the next section.

SECTION B

9.6 Analysis of Kalahari.net

Kalahari.net is a South African e-commerce merchant that sells books, CDs, DVDs, wine, software and electronic goods (figure 9.8). On the home page (figure 9.9) there is evidence of the security features being used. A logo and link are provided for Thawte. The user is also informed that all payments are processed by ABSA. Logos are also given for eBucks, Standard Bank and icanonline. All of this information helps to associate Kalahari.net with reputable companies. Even before the user has purchased anything, they are being reassured of their online security.

For the purpose of this dissertation a book was bought from Kalahari.net.



kalahari.net ® James's shop! contact us help

WELCOME | BOOKS | KICKBACKCLUB | TERTIARY BOOKS | SCHOOLBOOKS | SA GATEWAY | LIFESTYLE | HEALTH | VERIMARK | WINE

DVD / VIDEO | MUSIC | GAMING | SOFTWARE | PHOTOGRAPHY | TRAVEL | MAGAZINES | COURIER | AIRTIME | makro | Computicket

SEARCH: All products | SIGN IN | MY BASKET | MY PROFILE | MY ORDERS

First time @ Kalahari? Sign up now! | Need a corporate account? Sign up now! | Become an e-Trader - join now | Terms & Conditions

Minki Book Project more info

Seil in Afrikaans!

Site Map
- WELCOME
- AIRTIME
- BOOKS
  - Afrikaans
  - BBC Food
  - Bestsellers
  - Business
  - Christianity
  - Computers
  - Fiction
  - Harry Potter
  - Kids' Corner
  - New Releases
  - Sexual Wellbeing
  - SF & Fantasy
  - Soul Food
  - The Tolkien Room
- COMPETITIONS
- COMPUTICKET

Welcome, James Johnston!

20% Off ALL Music

School of Rock Original Soundtrack Was R136.95, now R109.56	In the Zone Britney Spears Was R210.95, now R168.76	The Blue Jukebox Chris Rea Was R136.95, now R109.56
» Soundtrack noise	» Best DVD noise	» Blues noise

Laduuuuma! SA scores World Cup.

2010 FIFA

Well done SA on winning the bid to host 2010 Soccer World Cup. Check out the latest and greatest soccer paraphernalia here.

In my basket
1. The Rich Dad's Guide To Investing (1)
add to wishlist | remove
TO CHECKOUT

My wishlists - NEW!
1. Lord Of The Rings - Fellowship Of The Ring
put in basket | remove

How to join the kickbackclub

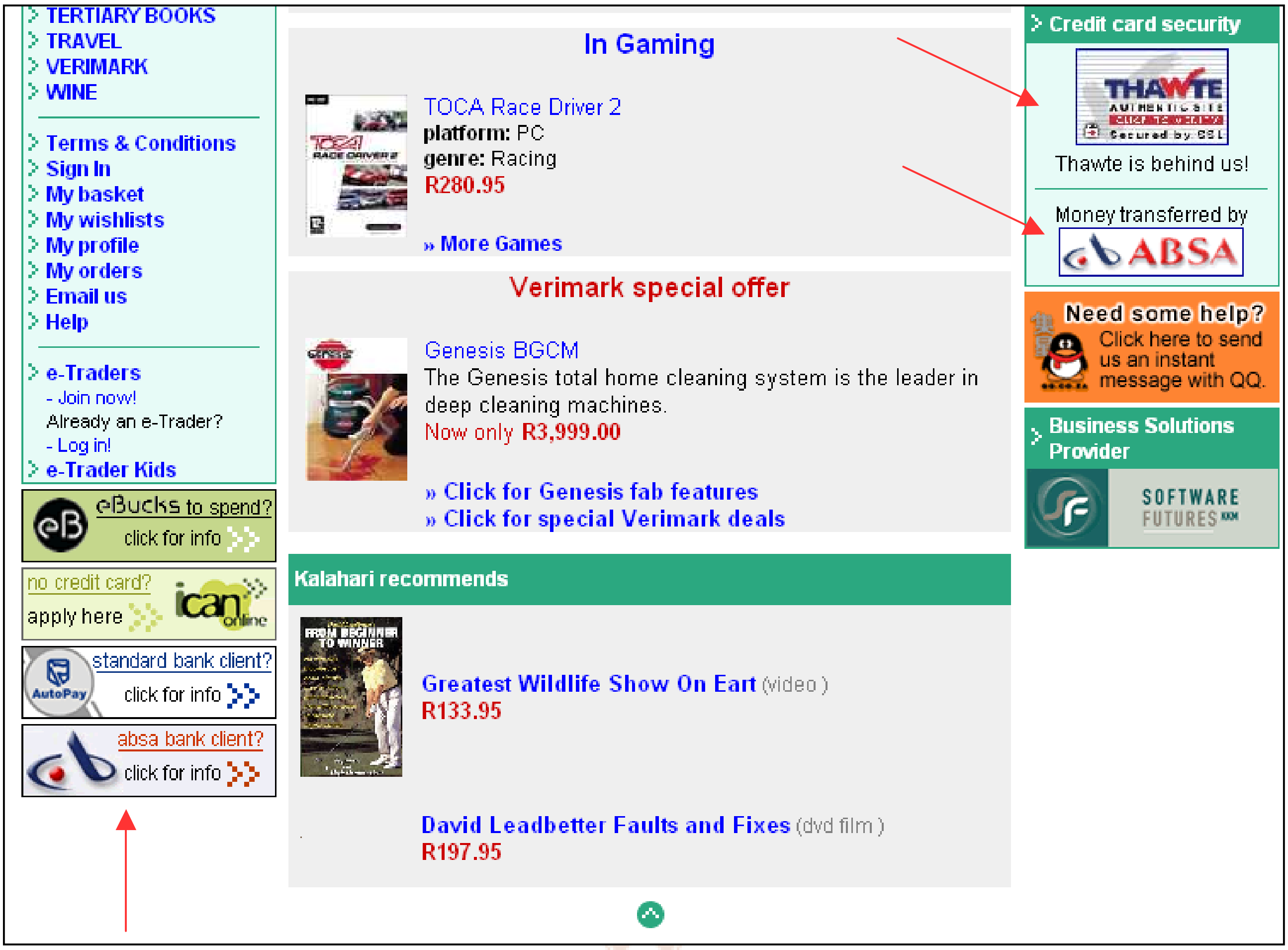
How to enjoy personal recommendations

Send an e-voucher

Send a wrapped gift

looking for a job??
Kalahari.net is looking for a music editor

Fig 9.8 Home page part 1



TERTIARY BOOKS
TRAVEL
VERIMARK
WINE

Terms & Conditions
Sign In
My basket
My wishlists
My profile
My orders
Email us
Help

e-Traders
- Join now!
Already an e-Trader?
- Log in!
e-Trader Kids

eBucks to spend? click for info

no credit card? apply here ican online

standard bank client? click for info

absa bank client? click for info

In Gaming

TOCA Race Driver 2
platform: PC
genre: Racing
R280.95

» More Games

Verimark special offer

Genesis BGCM
The Genesis total home cleaning system is the leader in deep cleaning machines.
Now only R3,999.00

» Click for Genesis fab features
» Click for special Verimark deals

Kalahari recommends

Greatest Wildlife Show On Eart (video)
R133.95

David Leadbetter Faults and Fixes (dvd film)
R197.95

Credit card security

Thawte is behind us!

Money transferred by ABSA

Need some help? Click here to send us an instant message with QQ.

Business Solutions Provider

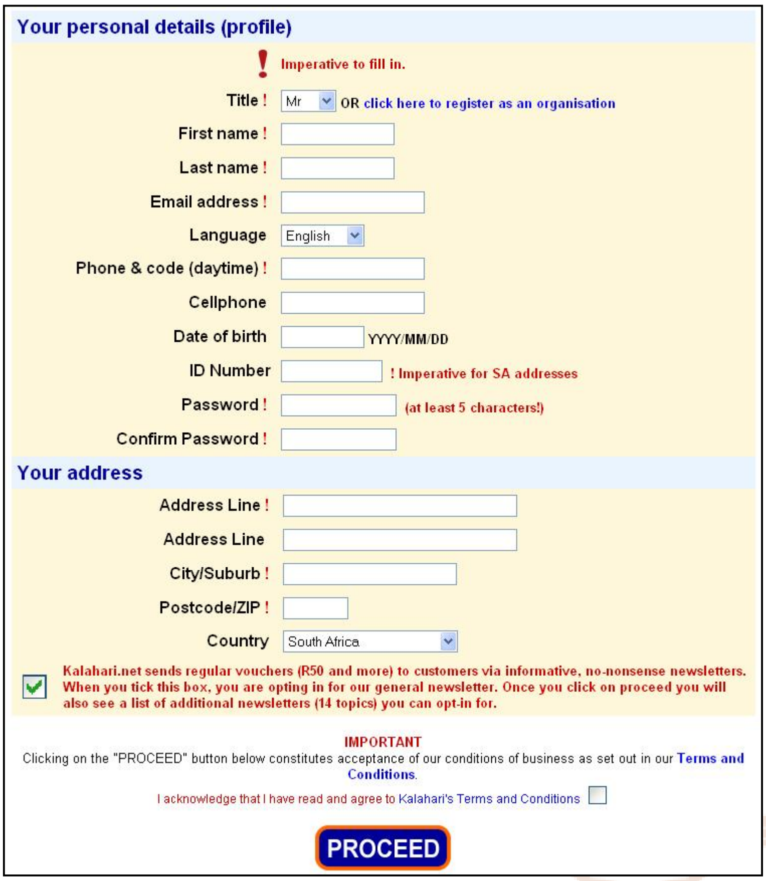
SOFTWARE FUTURES

Fig 9.9 Home page part 2

9.6.1 Compulsory registration

In order to purchase any item from Kalahari.net it is compulsory to register. This helps to make future purchases quicker. However, it can also be a disadvantage to a user who just wants to buy something quickly. An email address is used as a username (figure 9.10). The user is asked to choose a password which is at least five characters long. However, other instructions for choosing a secure password are not given (see chapter 7, 7.6.2 for examples of possible instructions).

The user is not informed of Kalahari.net's privacy policy on the registration page. The user is told that it is "imperative" for them to provide their ID number. However, they are not told why. A short sentence such as "*Kalahari.net will not sell or distribute your private information*" would go along way towards reassuring customers. Instead, the user needs to go to the help function to find out what Kalahari.net does with a user's private information. Information on the registration page is protected by SSL, but the user is not informed of this.



Your personal details (profile)

! Imperative to fill in.

Title !	Mr OR click here to register as an organisation
First name !	
Last name !	
Email address !	
Language	English
Phone & code (daytime) !	
Cellphone	
Date of birth	YYYY/MM/DD
ID Number	! Imperative for SA addresses
Password !	(at least 5 characters!)
Confirm Password !	

Your address

Address Line !	
Address Line	
City/Suburb !	
Postcode/ZIP !	
Country	South Africa

☑ Kalahari.net sends regular vouchers (R50 and more) to customers via informative, no-nonsense newsletters. When you tick this box, you are opting in for our general newsletter. Once you click on proceed you will also see a list of additional newsletters (14 topics) you can opt-in for.

IMPORTANT

Clicking on the "PROCEED" button below constitutes acceptance of our conditions of business as set out in our Terms and Conditions.

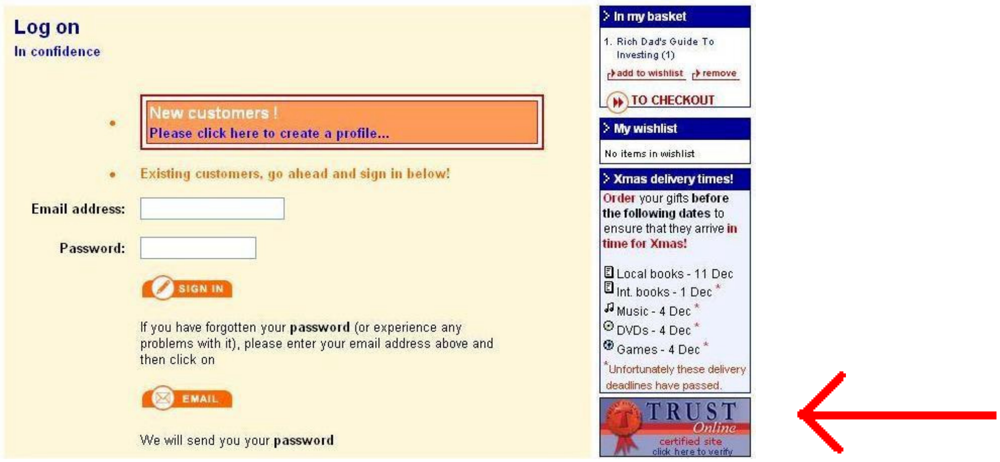
I acknowledge that I have read and agree to Kalahari's Terms and Conditions □

Fig 9.10 Registration

The passwords/login component is analysed in the next section.

9.6.2 Use of passwords/login

The login page has an *Aesthetic and minimalist design*. The page is predictable and most users should not have any problems logging in. After a successful login a user is welcomed. Kalahari.net has been endorsed by an independent third party – Trust Online. Trust Online's logo can be found at the bottom right-hand corner of the login page (figure 9.11). Trust Online is a South African e-commerce legal compliance certification and online dispute resolution service aimed at encouraging e-commerce by creating trust between the e-tailer and the public [TRUST02]. An unsure user is able to click on the logo and find out more about Trust Online and how it protects consumers' interests.



Log on
In confidence

- New customers !
  Please click here to create a profile...
- Existing customers, go ahead and sign in below!

Email address:

Password:

SIGN IN

If you have forgotten your **password** (or experience any problems with it), please enter your email address above and then click on

EMAIL

We will send you your **password**

In my basket

1. Rich Dad's Guide To Investing (1)

add to wishlist remove

TO CHECKOUT

My wishlist

No items in wishlist

Xmas delivery times!

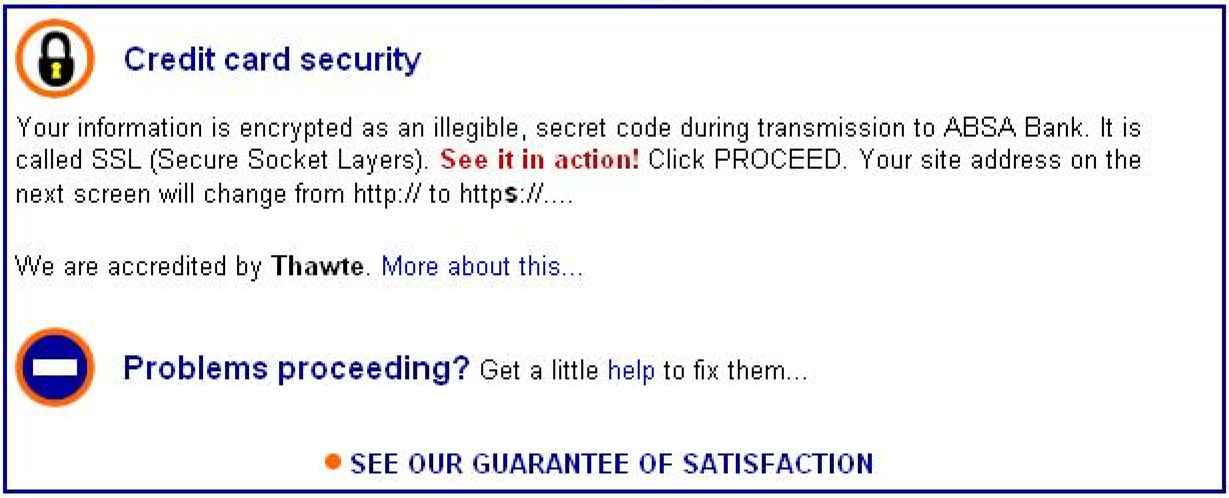
Order your gifts before the following dates to ensure that they arrive in time for Xmas!

Local books - 11 Dec
Int. books - 1 Dec *
Music - 4 Dec *
DVDs - 4 Dec *
Games - 4 Dec *
*Unfortunately these delivery deadlines have passed.

Fig 9.11 Log on

9.6.3 SSL – secure connections

Kalahari.net uses encryption during the logon and payment processes. On the logon page the user's attention is not drawn to this fact. However, when it comes to entering in credit card details, the user is informed that SSL is being used to ensure that the transaction is secure (figure 9.12). The user is able to follow links to more information on security and view Kalahari.net's guarantee (described in section 9.6.6). 'https' and the browser padlock are visible whenever SSL is being used at Kalahari.net.



Credit card security

Your information is encrypted as an illegible, secret code during transmission to ABSA Bank. It is called SSL (Secure Socket Layers). **See it in action!** Click PROCEED. Your site address on the next screen will change from http:// to https://....

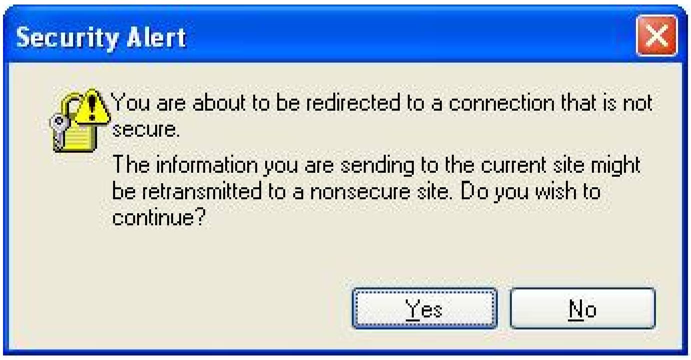
We are accredited by **Thawte**. More about this...

Problems proceeding? Get a little help to fix them...

● SEE OUR GUARANTEE OF SATISFACTION

Fig 9.12 Credit card security

The *Visibility of system status* is clear throughout the ordering process. The user is clearly informed of the steps in the process and warned against using the 'back button' on their browser. When the order has been completed the following warning is displayed: *"Some browsers may issue a security warning when you return to the site. Your transaction has been securely executed! Ignore the warning and you will return to the non-secure site* *without risking the secrecy of your credit card details."* This comment helps to put at ease any concerns a user may have about the security alert shown in figure 9.13.



Security Alert

You are about to be redirected to a connection that is not secure.

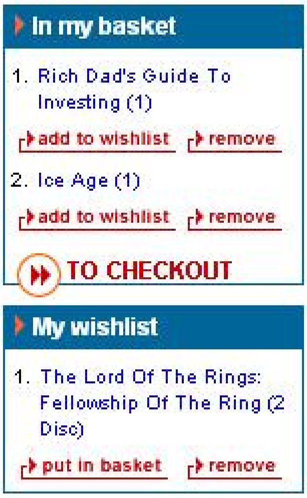
The information you are sending to the current site might be retransmitted to a nonsecure site. Do you wish to continue?

Fig 9.13 Security alert – Internet Explorer

9.6.4 Shopping cart and checkout

Kalahari.net stores the items a user chooses in a 'basket' (figure 9.14). A wishlist is also provided for items which a user may want in the future. The basket has an *Aesthetic and minimalist design* and behaves in a predictable manner. It is easy to add and remove items from the basket. The basket is similar to other shopping carts found at other e-commerce merchants, such as *Amazon.com,* which means that a user may already be familiar with the basket. This aids the *Learnability* of the basket.

One frustration, as can be seen from figure 9.14, is that the basket does not show the prices of the items selected so far. This decreases the *Satisfaction* as the user is not sure how much the items are going to cost them and if they could afford another item.



In my basket

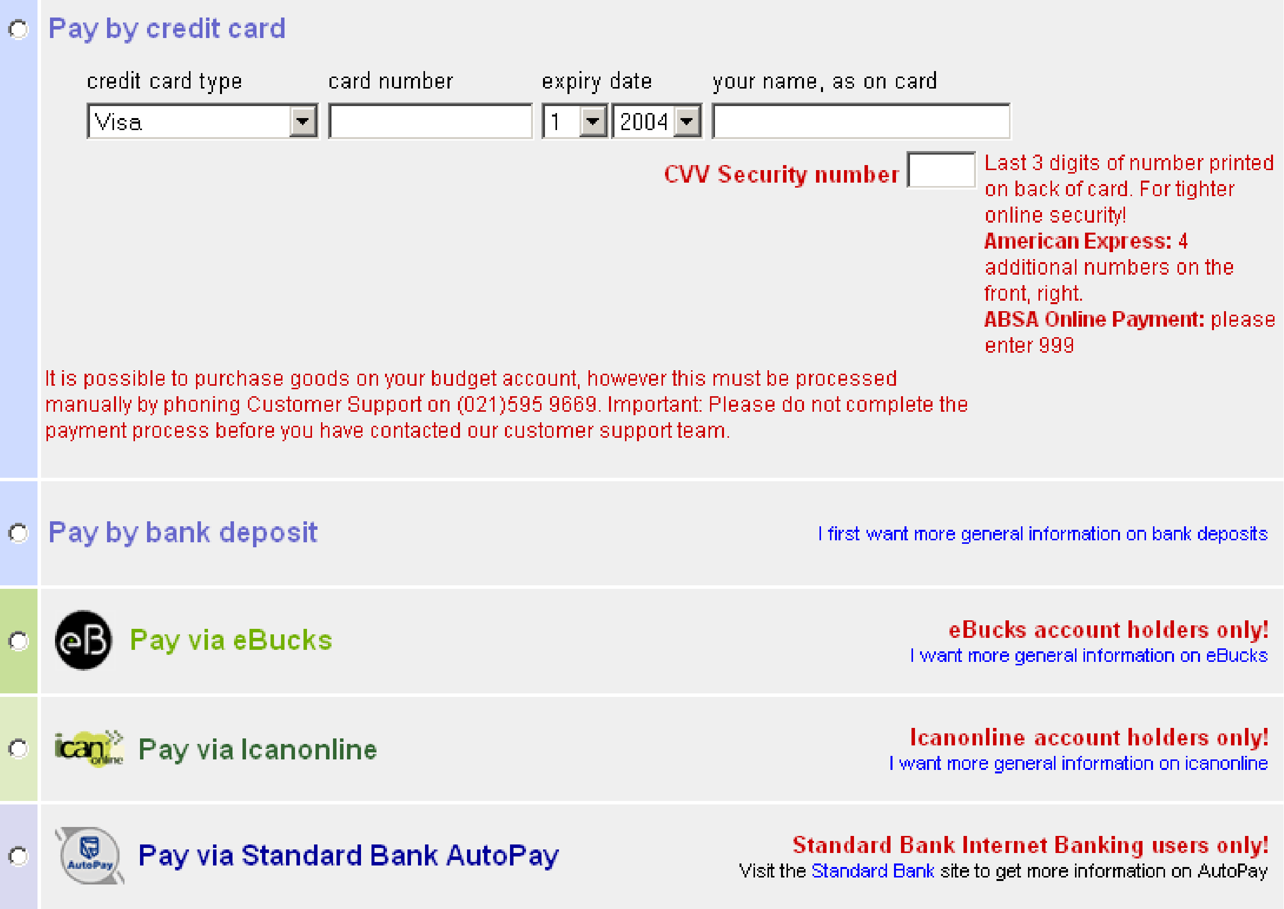
1. Rich Dad's Guide To Investing (1)
2. Ice Age (1)

My wishlist

1. The Lord Of The Rings: Fellowship Of The Ring (2 Disc)

Fig 9.14 Shopping cart and wishlist

Once the user has added items to their basket, they can proceed to the payment page by clicking 'To checkout'. As was seen in the analysis of the SSL component, the user is informed that transactions conducted are secure and that SSL is being used (figure 9.12). The user is also given a number of different payment options shown in figure 9.15. This helps the user to feel in control as they are able to choose the most convenient payment option. The user is also able to choose the payment option which they trust the most.



○ Pay by credit card

credit card type	card number	expiry date	your name, as on card
Visa		1 2004	

CVV Security number

Last 3 digits of number printed on back of card. For tighter online security!
American Express: 4 additional numbers on the front, right.
ABSA Online Payment: please enter 999

It is possible to purchase goods on your budget account, however this must be processed manually by phoning Customer Support on (021)595 9669. Important: Please do not complete the payment process before you have contacted our customer support team.

○ Pay by bank deposit

I first want more general information on bank deposits

○ Pay via eBucks

eBucks account holders only!
I want more general information on eBucks

○ Pay via Icanonline

Icanonline account holders only!
I want more general information on icanonline

○ Pay via Standard Bank AutoPay

Standard Bank Internet Banking users only!
Visit the Standard Bank site to get more information on AutoPay

Fig 9.15 Various payment options

9.6.5 Logout button

Kalahari.net does not have a logout/logoff button. This is a huge oversight. Kalahari.net uses cookies to track the users. This means that the next time a user logs on to Kalahari.net, they are greeted by name and any existing items in their basket and wishlist are shown. Previously (year 2003) anyone who visited Kalahari.net from the same computer would have had access to the previous user's:

- shopping basket
- wishlist

- shopping preferences
- first name and surname
- telephone number
- address
- birthday
- ID number

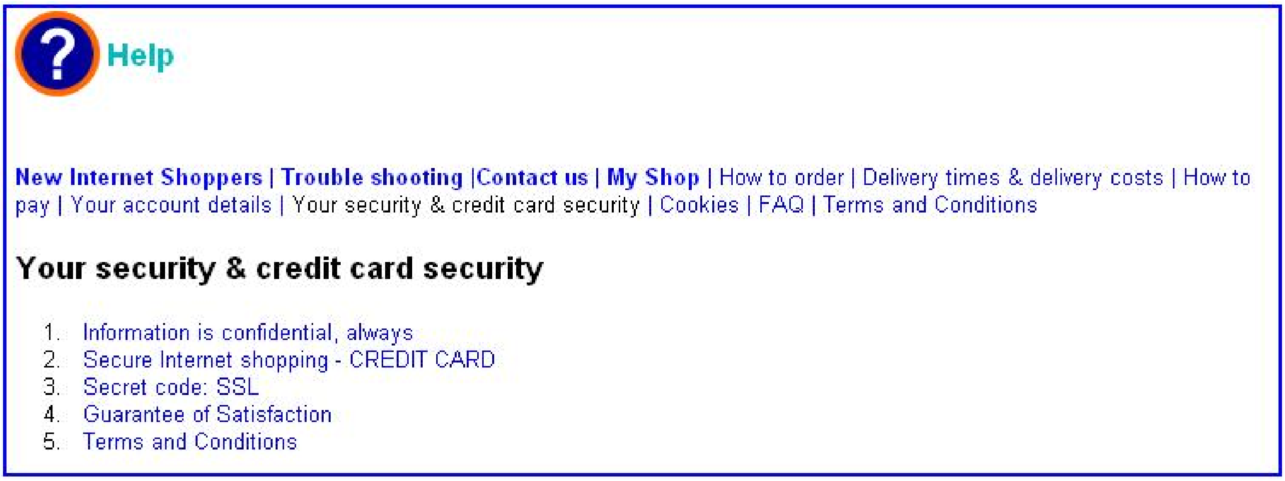
Kalahari.net has fixed this security breach and a user now needs to enter their email address and password in order to access personal details. A simple logoff button would have avoided this problem.

9.6.6 Online help

Kalahari.net offers an extensive help function on all aspects of online shopping. The help function is easy to access and navigate. In some cases the help is context-sensitive.

Help on security issues is provided under the heading of "Your security & credit card security" (figure 9.16). The following topics are dealt with:

1. Information is confidential, always
2. Secure Internet shopping - CREDIT CARD
3. Secret code: SSL
4. Guarantee of Satisfaction
5. Terms and Conditions



New Internet Shoppers | Trouble shooting |Contact us | My Shop | How to order | Delivery times & delivery costs | How to pay | Your account details | Your security & credit card security | Cookies | FAQ | Terms and Conditions

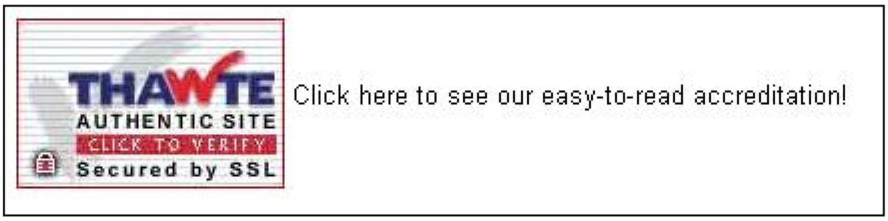
Your security & credit card security

1. Information is confidential, always
2. Secure Internet shopping - CREDIT CARD
3. Secret code: SSL
4. Guarantee of Satisfaction
5. Terms and Conditions

Fig 9.16 Online help

Topic 1 discusses Kalahari.net's privacy policy. Topic 2 explains to the user that ABSA handles the transfer of money for Kalahari.net. Kalahari.net is also an approved credit card operator for ABSA. This third-party endorsement by ABSA helps lend credibility to Kalahari. This increases the *Trust* that a user would have in Kalahari.net.

Topic 3 briefly explains what SSL is to the user and what the benefits of SSL are. A Thawte logo (figure 9.17) and link are provided for the user to verify that Kalahari.net are who they say they are. From chapter 7 (section 7.4.1) it was seen that seals of approval, like Thawte, assist in developing *Trust* between a website and the user. Kalahari.net ensures that these seals are *conveyed* to the user.



THAWTE
AUTHENTIC SITE
CLICK TO VERIFY
Secured by SSL

Click here to see our easy-to-read accreditation!

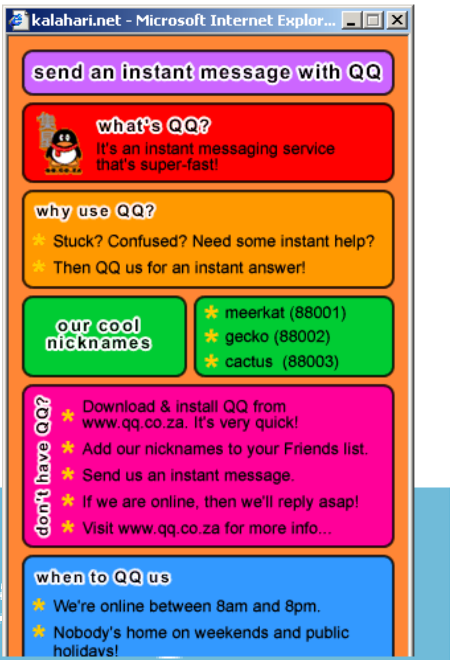
Fig 9.17 Third-party endorsement

Topic 4 provides a guarantee that if a fraudulent transaction does occur on the user's credit card, Kalahari.net will refund the user up to R500. Topic 5 discusses the terms and conditions of using the Kalahari.net website.

Kalahari.net also offers a live chat help feature using the free QQ instant messenger (figure 9.18).

Fig 9.18 QQ instant messenger

Between 8am and 8pm during the week a user can login to QQ and ask for assistance. This helps to raise the level of *Trust* as a user is able to obtain real-time assistance.



kalahari.net - Microsoft Internet Explor...

send an instant message with QQ

what's QQ?
It's an instant messaging service that's super-fast!

why use QQ?
- Stuck? Confused? Need some instant help?
- Then QQ us for an instant answer!

our cool nicknames
- meerkat (88001)
- gecko (88002)
- cactus (88003)

don't have QQ?
- Download & install QQ from www.qq.co.za. It's very quick!
- Add our nicknames to your Friends list.
- Send us an instant message.
- If we are online, then we'll reply asap!
- Visit www.qq.co.za for more info...

when to QQ us
- We're online between 8am and 8pm.
- Nobody's home on weekends and public holidays!

However, the user first has to download the QQ software. Giving the user the option to use a more popular instant chat program, such as Microsoft Messenger, would remove some of the hassle.

9.7 Conclusion of Kalahari.net analysis

The analysis of each component is presented in table format. Table 9.3 provides an explanation of the colours used.

9.7.1 Registration

A summary of the analysis of the registration component is provided in the following table:

Table 9.10 Registration

Criteria	***Conclusion***	***Impact***	
Convey features (16.6% weighting)	**Partial** The user is not directly informed of the privacy policy. User is told certain fields are imperative, but not told why. User is not encouraged to choose a secure password.	User may be hesitant to provide personal details.	8.3%
Visibility of system status (16.6% weighting)	**Partial** The user is not directly informed that their personal information is being protected by SSL.	User may provide incorrect personal details.	8.3%
Learnability (16.6% weighting)	**Partial** Email address used for username. Only limited password requirements are displayed.	User may choose a password which is insecure.	8.3%
Aesthetic and minimalist design (16.6% weighting)	**YES** Simple and clean interface. User is not asked for too much information.	Form is quick and easy to complete.	16.6%
Errors (16.6% weighting)	**YES** Error messages are clear.	Most users should understand error messages.	16.6%
Satisfaction (16.6% weighting)	**YES** Telephone number and an email address are given.	User is able to obtain assistance if needed.	16.6%

Criteria	***Conclusion***	***Impact***	
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 75% level of trust has been developed.	**Total**	**75%**

Kalahari.net meets three of the criteria and partially meets the three remaining criteria. The main reason why Kalahari.net has not completely met all the criteria is the lack of a policy.

9.7.2 Use of passwords/login

The passwords/login component is summarised in the following table:

Table 9.11 Passwords/login component

Criteria	***Conclusion***	***Impact***	
Convey features (16.6% weighting)	**YES** User is informed that they can 'log on in confidence'. Clicking on 'Confidence' link displays information on security. Login page has a third-party endorsement from Trust Online.	User will understand that precautions are being taken to ensure the security of their transaction.	16.6%
Visibility of system status (16.6% weighting)	**Partial** Status of SSL is conveyed by the small padlock in Internet Explorer. User's attention is not directly drawn to SSL.		8.3%
Learnability (16.6% weighting)	**YES** Email address has been used as a username.	User will probably not forget their email address.	16.6%
Aesthetic and minimalist design (16.6% weighting)	**YES** Page loads quickly and has a simple design.	User will be able to login quickly.	16.6%
Errors (16.6% weighting)	**Partial** Usability of site is enhanced by informing the user of whether their username or their password was entered incorrectly.	Site's security is reduced by providing this additional information.	8.3%

Criteria	*Conclusion*	*Impact*	
Satisfaction (16.6% weighting)	**YES** It is quick and easy for a user to reset a forgotten password.	First-time users should feel confident logging in. Users who login frequently will not be hassled with additional information and long download times.	16.6%
Does the interface lead to trust being developed?			
Trust (100% weighting)	An 83% level of trust has been developed.	**Total**	**83%**

Kalahari.net scores highly in the passwords/login component. The correct balance between HCI and security has been achieved for this component.

9.7.3 SSL

The trust level of the SSL component, along with a summary, is provided in table 9.12.

Table 9.12 SSL component

Criteria	*Conclusion*	*Impact*	
Convey features (33.3% weighting)	**Partial** User is informed on the payment page that SSL is being used, that their credit card is secure and that Kalahari.net has been accredited by Thawte. However, the user is not informed of the use of SSL on the registration and login pages.	User may not be aware that SSL is being used on the registration and login pages.	16.6%
Visibility of system status (33.3% weighting)	**YES** Status of SSL is conveyed by the small padlock in Internet Explorer and by messages on the payment page.	User will feel confident providing their credit card details.	33.3%
Learnability	Not applicable.	Not applicable.	
Aesthetic and minimalist design	Not applicable.	Not applicable.	
Errors	Not applicable.	Not applicable.	

Criteria	*Conclusion*	*Impact*	
Satisfaction (33.3% weighting)	**YES** The user will be aware that steps are being taken to ensure the safety of transactions.	The user may initially be hesitant to provide personal information on the registration page.	33.3%
Does the interface lead to trust being developed?			
Trust (100% weighting)	An 83% level of trust has been developed.	**Total**	**83%**

Kalahari.net scores highly in the SSL component. This is mainly because the user is informed in a simple and easy-to-understand manner of the implementation of SSL (figure 9.12). The Thawte accreditation also helps to make the user aware of the presence of SSL.

9.7.4 Shopping cart and checkout

Table 9.13 Shopping cart and checkout component

Criteria	*Conclusion*	*Impact*	
Convey features (20% weighting)	**YES** User is informed that SSL is being used and that Kalahari.net has been accredited by Thawte.	User will be aware that security measures are being taken to protect their transaction.	20%
Visibility of system status (20% weighting)	**YES** Status of SSL is conveyed by the small padlock in Internet Explorer and by messages on the payment page.	User will feel confident providing their credit card details.	20%
Learnability (20% weighting)	The user is guided through the checkout process.	Users who have shopped at other e-tailers will find the shopping basket familiar.	20%
Aesthetic and minimalist design (20% weighting)	**YES** Checkout process is split among a number of pages. This means that the user is not swamped with information.	User will find the checkout process quick and easy.	20%
Errors	An environment which generated errors could not be created.		

Criteria	*Conclusion*	*Impact*	
Satisfaction (20% weighting)	**Partial** The user will be aware that steps are being taken to ensure the safety of transactions. The prices of items in the shopping basket are not visible.	The user will be frustrated that they cannot easily see the total cost of the items in the basket.	10%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 90% level of trust has been developed.	**Total**	**90%**

Kalahari.net develops a high level of trust with regard to the shopping cart and checkout component. Many parts of the checkout process make use of SSL. As was seen previously, Kalahari.net obtained a high score for the SSL component. The high SSL score in turn has a positive influence on the shopping cart and checkout component's level of trust.

9.7.5 Online help

The online help summary follows in table 9.14.

Table 9.14 Online help

Criteria	*Conclusion*	*Impact*	
Convey features (25% weighting)	**Partial** SSL, Thawte and Trust Online are explained in an easily understandable manner in the help file. Topics such as spyware and anti-virus software are not mentioned, however.	Reading the help file will lead to an increase in the level of trust.	12.5%
Visibility of system status	Not applicable.	Not applicable.	
Learnability (25% weighting)	**YES** Help is broken down into logical components. User is not provided with too much technical information.	Most users should be able to understand the help component.	25%
Aesthetic and minimalist design (25% weighting)	**YES** Navigation bar is provided.	User should be able to find what they are looking for.	25%

Criteria	*Conclusion*	*Impact*	
Errors	Not applicable.	Not applicable.	
Satisfaction (25% weighting)	**YES** Additional assistance is provided via QQ instant messaging.	Most queries and concerns which a user has should be answered by the help component.	25%
Does the interface lead to trust being developed?			
Trust (100% weighting)	An 88% level of trust has been developed.	**Total**	**88%**

Kalahari.net has a comprehensive online help facility. There are, however, some current topics such as spyware and phishing which need to be included. A facility to search the help would also be beneficial for users.

Overall Kalahari.net scores:

75%	registration
83%	passwords/login
83%	SSL
90%	shopping cart and checkout
88%	online help

giving an average level of trust of 84%.

The interface of Kalahari.net scores well from an HCI-S perspective. Only the registration component scores below the eighties. A number of small changes can, however, be made to improve this score. These modifications are discussed in the next section.

9.8 Recommendations for Kalahari.net

Recommendations on how the level of trust can be improved are discussed in this section. Recommendations are made for each of the components.

9.8.1 Recommendations for registration component

The first recommendations are for the registration component and follow in table 9.15.

Table 9.15 Registration component

Criteria	***Recommendation***	***Conclusion after recommendation***	***Proposed score***
Convey features (33.3% weighting)	Briefly inform the user of Kalahari.net's privacy policy on the registration page.	**YES** User will be aware that their personal information is secure.	33.3%
Visibility of system status (33.3% weighting)	Inform the user that all personal information that is transferred over the Internet is protected by SSL.	**YES** Users will register with confidence.	33.3%
Learnability	Encourage the user to choose a secure password. Show the user an example of a password or pass phrase.	**YES** User will hopefully choose a password that cannot be cracked easily.	33.3%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 100% level of trust has been developed.	**Total**	**Proposed: 100%** **Existing: 75%**

A number of modifications to the registration component can see the level of trust grow substantially.

9.8.2 Recommendations for passwords/login

Recommendations relating to two of the HCI-S criteria are made in the following table:

Table 9.16 Passwords/login component

Criteria	***Recommendation***	***Conclusion after recommendation***	***Proposed score***
Visibility of system status (33.3% weighting)	Inform the user of the use of SSL on the login page. Perhaps also include a 'Thawte accreditation' link. Inform the user of the date and time of their last login.	**YES** User will login with confidence.	16.6%
Errors	**Partial** In order to maintain a balance between security and usability it is recommended that the error messages remain the same.		8.3%

Criteria	*Recommendation*	*Conclusion after recommendation*	*Proposed score*
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 91% level of trust has been developed.	**Total**	**Proposed: 91%** **Existing: 83%**

It is not recommended that Kalahari.net aim for a 100% level of trust with regard to the passwords/login component. This level of trust is achievable, but it would negatively impact the usability of the site. The risks associated with the illegal access to a user's account do not necessitate a 100% level of trust. This is because the negative consequence of a hacker gaining access to a user's account is limited. The hacker would be unable to steal any money, but they would be able to gain access to some of the user's personal details. In a banking environment, where the consequences of a security breach are greater, a 100% score is recommended.

9.8.3 Recommendations for SSL component

One minor change to the SSL component can raise the level of trust to 100%.

Table 9.17 SSL component

Criteria	*Recommendation*	*Conclusion after recommendation*	*Proposed score*
Convey features (33.3% weighting)	Draw the user’s attention to the use of SSL on the login and registration pages.	**YES**	33.3%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 100% level of trust has been developed.	**Total**	**Proposed: 100%** **Existing: 83%**

9.8.4 Recommendations for shopping cart and checkout component

Including the price in the shopping basket will increase the user's level of satisfaction. Kalahari.net may have left out the prices on purpose, in order to encourage users to add more items to their shopping basket.

Table 9.18 Shopping cart and checkout component

Criteria	***Recommendation***	***Conclusion after recommendation***	***Proposed score***
Satisfaction	Display prices in shopping basket.	**YES** User will quickly be able to see predicted total.	20%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 100% level of trust has been developed.	**Total**	**Proposed: 100%** **Existing: 90%**

9.8.5 Recommendations for online help component

It appears that the current online help is dated. A number of current security threats need to be added to the help.

Table 9.19 Online help

Criteria	***Recommendation***	***Conclusion after recommendation***	***Proposed score***
Convey features (25% weighting)	Provide information on current security threats such as spyware. Also provide details on the importance of anti-virus software.	**YES** Users will feel confident that Kalahari.net is aware of the latest security threats.	25%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 100% level of trust has been developed.	**Total**	**Proposed: 100%** **Existing: 88%**

9.8.6 Recommendations for logout button component

Kalahari.net does not currently have a logout button. It is recommended that one be included. Clicking on the logout button will ensure that the session has been terminated and will help the user to feel more secure, leading to a higher level of trust.

As can be seen from table 9.20, Kalahari.net scores highly – 84% – with regard to trust. However, this level of trust can be improved to 98% with a number of minor modifications to the interface. Implementing these modifications will improve the user's online shopping experience and encourage new users, who may have security concerns, to shop from Kalahari.net.

Table 9.20 Overall score after recommendation

	Existing	***Proposed***
Registration	75%	100%
Passwords/login	83%	91%
SSL	83%	100%
Shopping cart and checkout	90%	100%
Online help	88%	100%
Average	**84%**	**98%**

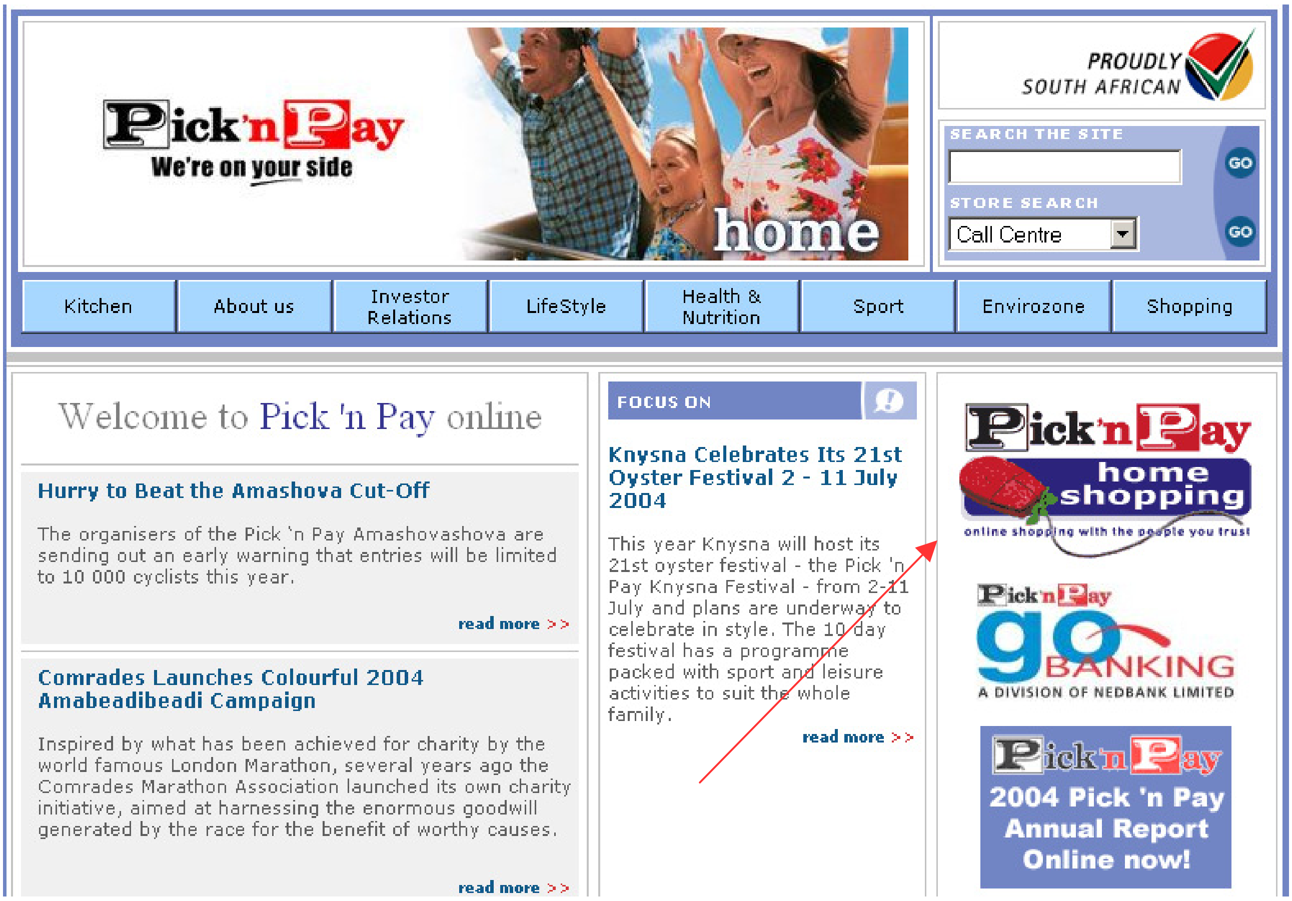
In the next section Picknpay.co.za is analysed.

SECTION C

9.9 Analysis of Picknpay.co.za

Pick 'n Pay is one of the leading retailers in South Africa. They have a turnover in excess of R29 billion (2003) and have been voted the most trusted company in South Africa in 2003 [CHAIR04]. Pick 'n Pay have developed a home shopping e-commerce website found at homeshopping.picknpay.co.za.

Figure 9.19 Shows the Pick 'n Pay home page. The text “online shopping with the people you trust” can be found below the home shopping logo. Pick 'n Pay is using their well known, and well trusted brand to foster trust online.



Welcome to Pick 'n Pay online

Hurry to Beat the Amashova Cut-Off

The organisers of the Pick 'n Pay Amashovashova are sending out an early warning that entries will be limited to 10 000 cyclists this year.

read more >>

Comrades Launches Colourful 2004 Amabeadibeadi Campaign

Inspired by what has been achieved for charity by the world famous London Marathon, several years ago the Comrades Marathon Association launched its own charity initiative, aimed at harnessing the enormous goodwill generated by the race for the benefit of worthy causes.

read more >>

Knysna Celebrates Its 21st Oyster Festival 2 - 11 July 2004

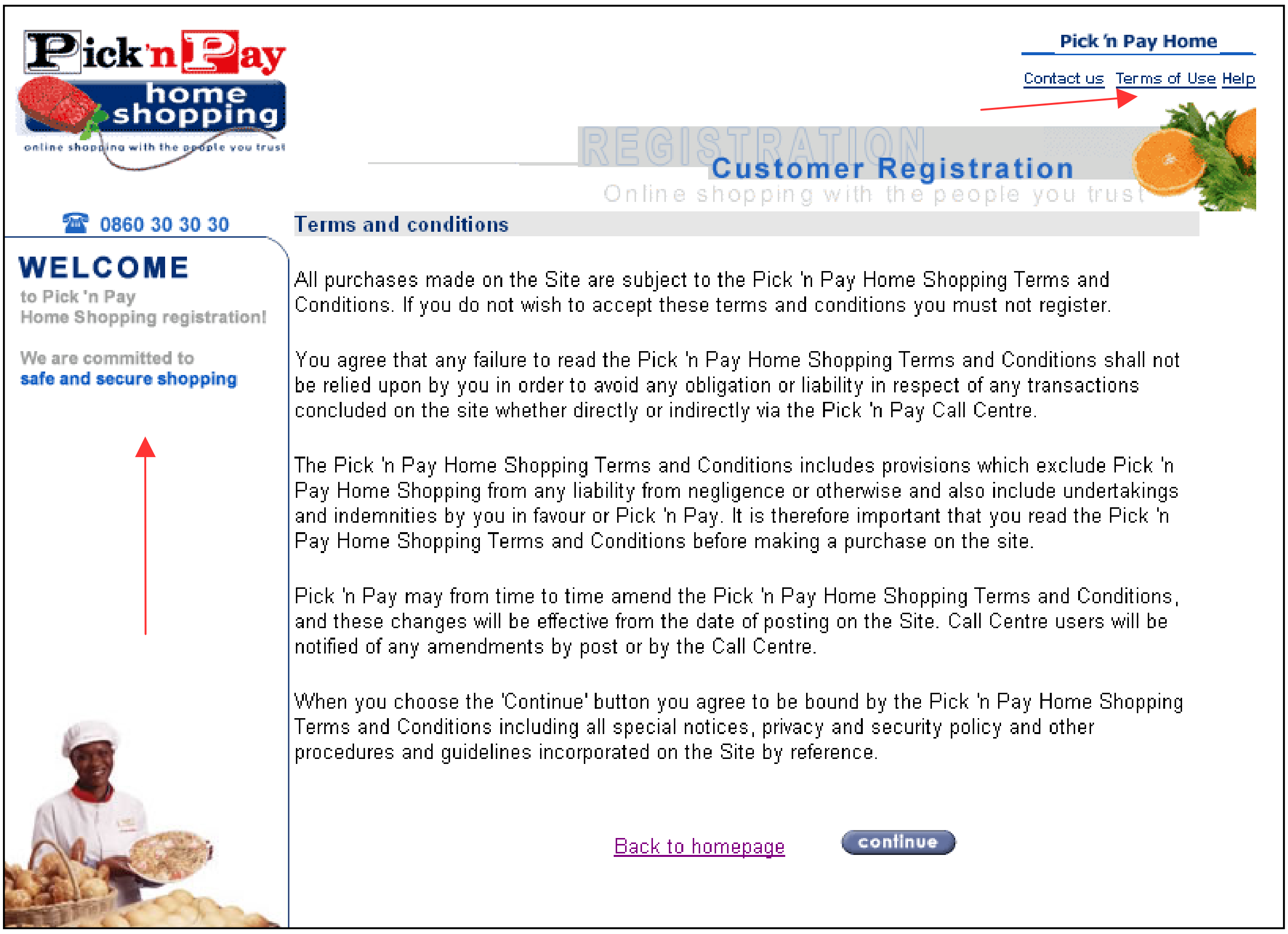
This year Knysna will host its 21st oyster festival - the Pick 'n Pay Knysna Festival - from 2-11 July and plans are underway to celebrate in style. The 10 day festival has a programme packed with sport and leisure activities to suit the whole family.

read more >>

Fig 9.19 Pick 'n Pay home page

9.9.1 Compulsory registration

In order to use Pick 'n Pay home shopping a user needs to register. Before a user can register they need to agree to the terms and conditions shown in figure 9.20. The user is reassured that Pick 'n Pay is 'committed to safe and secure shopping'. Clicking on the 'continue' button means that the user is bound by the privacy and security policy. However, the user is not at this stage informed of what that policy entails. To view the privacy and security policies the user must click on the 'Terms of Use' link (top right-hand corner of page).



Terms and conditions

All purchases made on the Site are subject to the Pick 'n Pay Home Shopping Terms and Conditions. If you do not wish to accept these terms and conditions you must not register.

You agree that any failure to read the Pick 'n Pay Home Shopping Terms and Conditions shall not be relied upon by you in order to avoid any obligation or liability in respect of any transactions concluded on the site whether directly or indirectly via the Pick 'n Pay Call Centre.

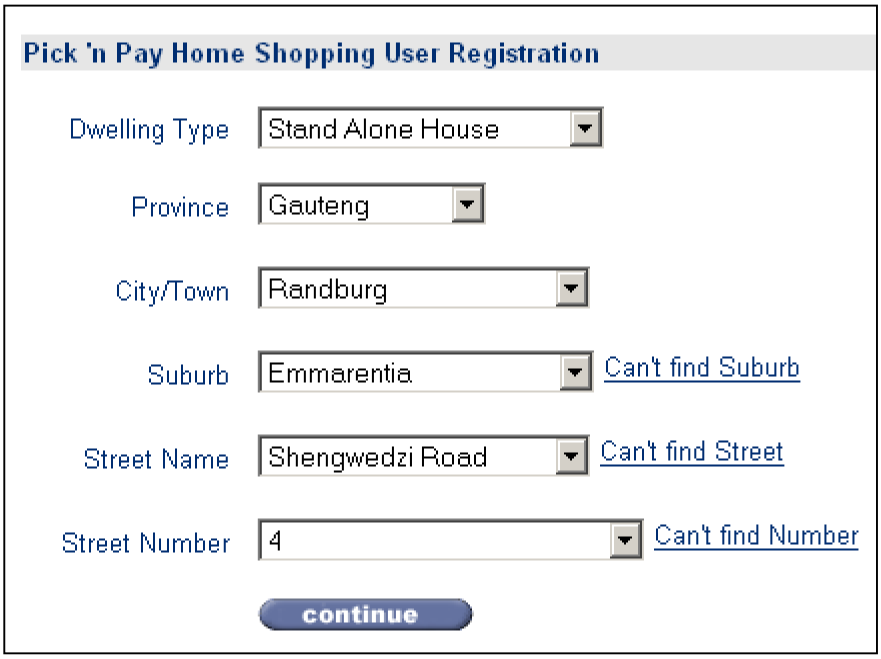
The Pick 'n Pay Home Shopping Terms and Conditions includes provisions which exclude Pick 'n Pay Home Shopping from any liability from negligence or otherwise and also include undertakings and indemnities by you in favour or Pick 'n Pay. It is therefore important that you read the Pick 'n Pay Home Shopping Terms and Conditions before making a purchase on the site.

Pick 'n Pay may from time to time amend the Pick 'n Pay Home Shopping Terms and Conditions, and these changes will be effective from the date of posting on the Site. Call Centre users will be notified of any amendments by post or by the Call Centre.

When you choose the 'Continue' button you agree to be bound by the Pick 'n Pay Home Shopping Terms and Conditions including all special notices, privacy and security policy and other procedures and guidelines incorporated on the Site by reference.

Fig 9.20 Registration

After clicking 'continue' the user is asked to choose their delivery address (figure 9.21). This is done by first choosing a province. Based on the province chosen, a list of relevant cities and towns is shown. Choosing a city causes only suburbs found in that city to be displayed. The same process is followed with the street name. Inputting an address in this format is quick and helps to ensure that the details in the address are correct.

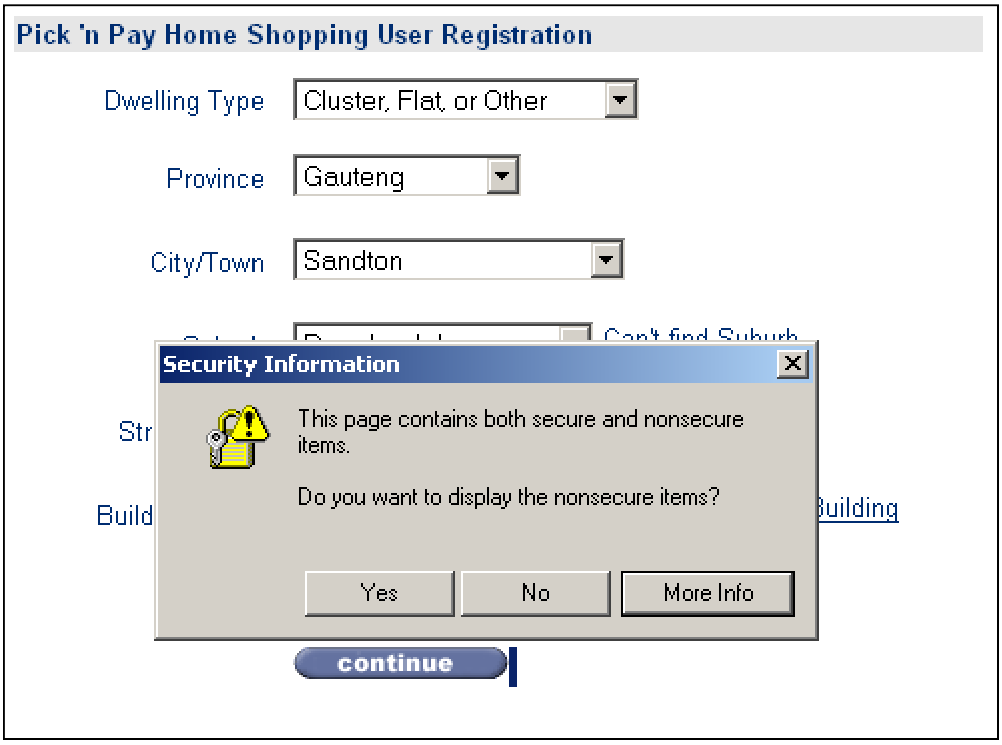


Pick 'n Pay Home Shopping User Registration

Dwelling Type	Stand Alone House	
Province	Gauteng	
City/Town	Randburg	
Suburb	Emmarentia	Can't find Suburb
Street Name	Shengwedzi Road	Can't find Street
Street Number	4	Can't find Number

Fig 9.21 Registration - address

Clicking on 'continue' causes the following standard Internet Explorer warning in figure 9.22 to be displayed. This is because the registration page uses frames (one web page made up of a number of other web pages). Only some of the frames use SSL, which causes the warning to be displayed. This error message may be quite confusing for a user. Unlike with Kalahari.net, the user is not warned that this message may be displayed.



Pick 'n Pay Home Shopping User Registration

Dwelling Type	Cluster, Flat, or Other
Province	Gauteng
City/Town	Sandton

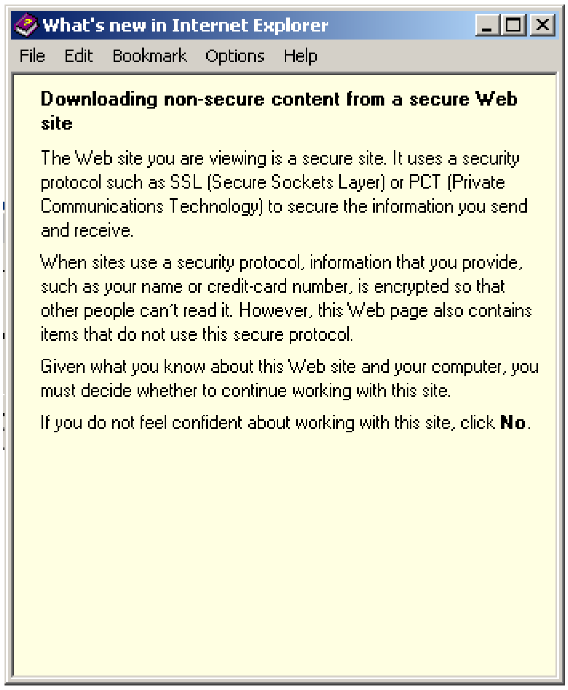
Security Information

This page contains both secure and nonsecure items.

Do you want to display the nonsecure items?

Fig 9.22 Warning

Clicking on 'More Info' provides an explanation of the meaning of this message. This explanation is shown in figure 9.23. As can be seen, this explanation is not easy for the average user to understand.


What's new in Internet Explorer
File Edit Bookmark Options Help

Downloading non-secure content from a secure Web site

The Web site you are viewing is a secure site. It uses a security protocol such as SSL (Secure Sockets Layer) or PCT (Private Communications Technology) to secure the information you send and receive.

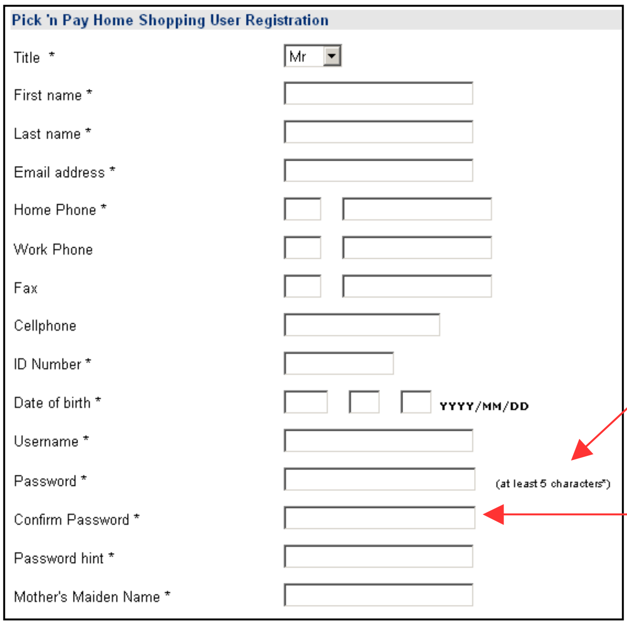
When sites use a security protocol, information that you provide, such as your name or credit-card number, is encrypted so that other people can't read it. However, this Web page also contains items that do not use this secure protocol.

Given what you know about this Web site and your computer, you must decide whether to continue working with this site.

If you do not feel confident about working with this site, click **No**.

Fig 9.23 Explanation of warning

After inputting the address the user is asked for their personal details (figure 9.24) including their ID number. The user is also asked for their password. The only instructions given are that the password must be at least five characters. The user is not told whether the password is case-sensitive nor encouraged to choose a secure password or pass phrase.



Pick 'n Pay Home Shopping User Registration

Title * Mr

First name *

Last name *

Email address *

Home Phone *

Work Phone

Fax

Cellphone

ID Number *

Date of birth * YYYY/MM/DD

Username *

Password * (at least 5 characters*)

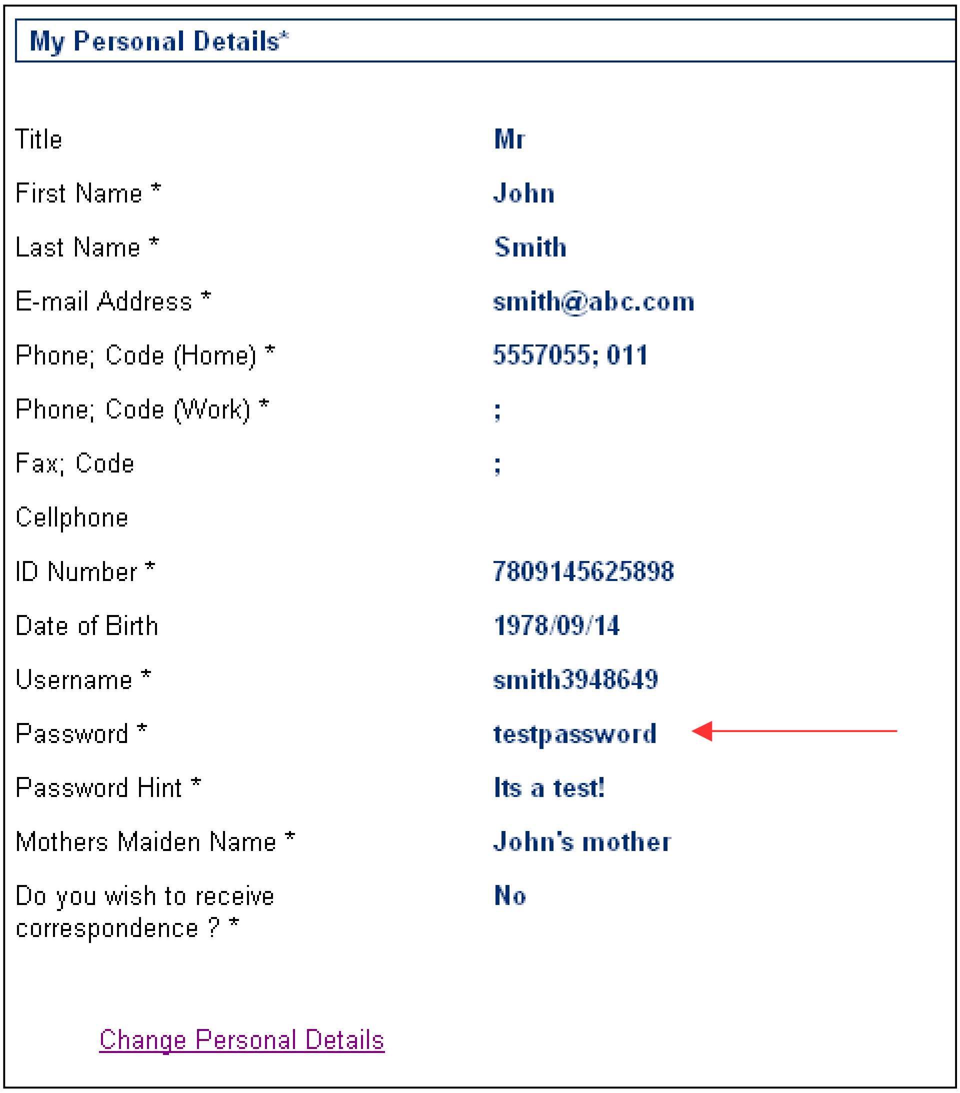
Confirm Password *

Password hint *

Mother's Maiden Name *

Fig 9.24 Registration – personal details

After entering all the details the user's information is displayed for confirmation (figure 9.25). This helps to ensure that all details have been captured correctly and helps to remind the user of the details entered. The user's password is shown in plain text. This aids the usability of the site as the user is less likely to forget their password if they are immediately reminded of it. However, this weakens the security of the system as someone looking over the user's shoulder may see the password. Pick 'n Pay obviously feel that this is a small risk and worth the added usability.



My Personal Details*

Title	Mr
First Name *	John
Last Name *	Smith
E-mail Address *	smith@abc.com
Phone; Code (Home) *	5557055; 011
Phone; Code (Work) *	;
Fax; Code	;
Cellphone	
ID Number *	7809145625898
Date of Birth	1978/09/14
Username *	smith3948649
Password *	testpassword
Password Hint *	Its a test!
Mothers Maiden Name *	John's mother
Do you wish to receive correspondence ? *	No

Fig 9.25 Registration - confirmation

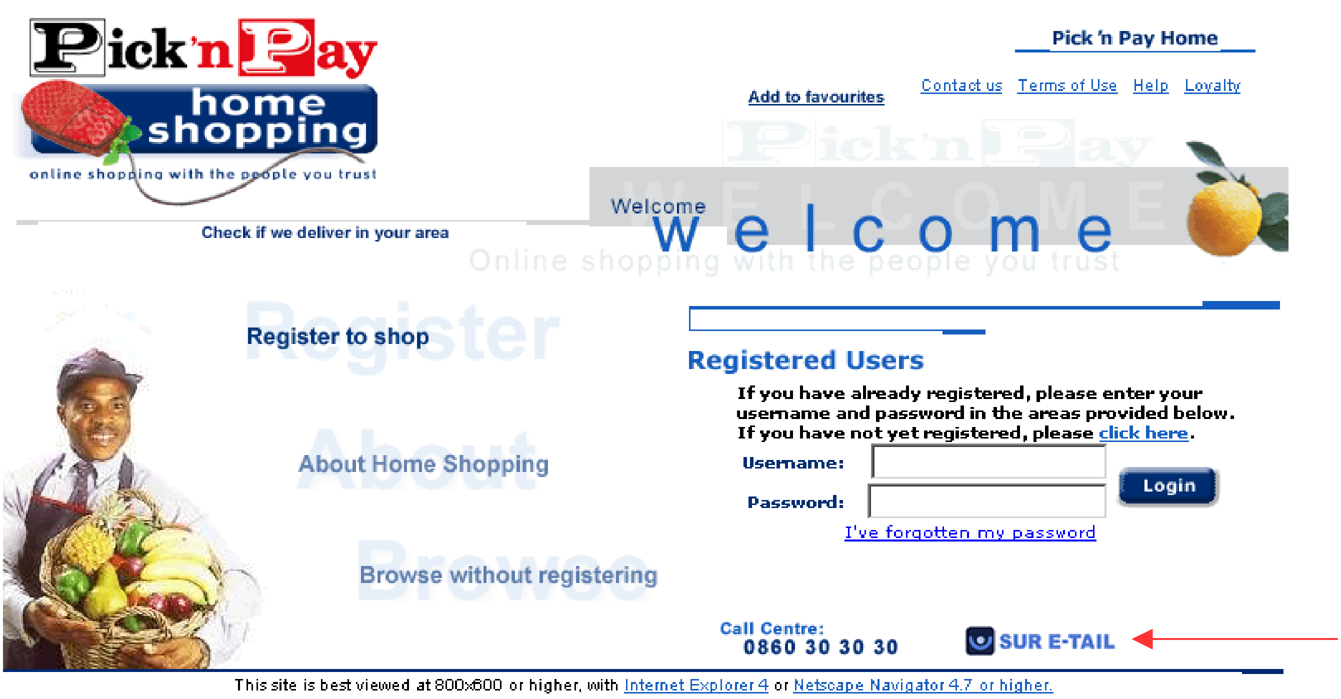
9.9.2 Use of passwords/login

Figure 9.26 shows the login page for Pick 'n Pay home shopping. The user is given the option to have their password sent to them if they forget it. However, they are not told what to do if they forget their username. Pick 'n Pay is a member of S.A.F.E. S.A.F.E. is an independent industry forum created by some of South Africa's leading online retailers.

The aim of S.A.F.E. is to promote the online shopping industry in South Africa. In order to help to achieve this members of S.A.F.E. have to:

- Guarantee encrypted transactions
- Uphold a published privacy policy
- Subscribe to the principles of permission-based marketing
- Adhere to a published refunds policy
- Display accurate contact details [SAFE04]

Online retailers who are members of S.A.F.E can display the SUR E-TAIL (figure 9.26) icon. However, Pick 'n Pay have not made the SUR E-TAIL icon on their login page clickable. Users are therefore not able to click on the icon for additional information. Users who recognise the icon will feel more secure and will trust the site. However, many users will not know what the icon is there for and what it means.



Pick'n Pay
home shopping
online shopping with the people you trust
Check if we deliver in your area
Pick 'n Pay Home
Add to favourites
Contact us
Terms of Use
Help
Loyalty
Welcome
welcome
Online shopping with the people you trust
Register to shop
About Home Shopping
Browse without registering
Login
I've forgotten my password
SUR E-TAIL

Registered Users

If you have already registered, please enter your username and password in the areas provided below. If you have not yet registered, please click here.

Username:

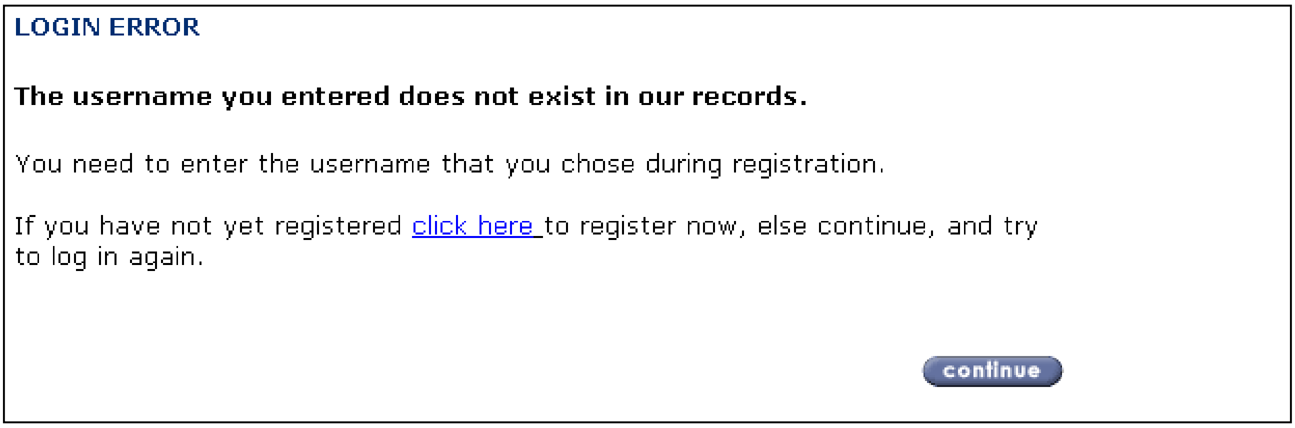
Password:

Call Centre: 0860 30 30 30

This site is best viewed at 800x600 or higher, with Internet Explorer 4 or Netscape Navigator 4.7 or higher.

Fig 9.26 Login for Picknpay.co.za

Entering the incorrect username generates the error message shown in figure 9.27. This message does not assist users who have forgotten their username. Perhaps an option could have been given for the user to enter their email address which they used at registration. The email address could then be used to look up the user's username.



LOGIN ERROR

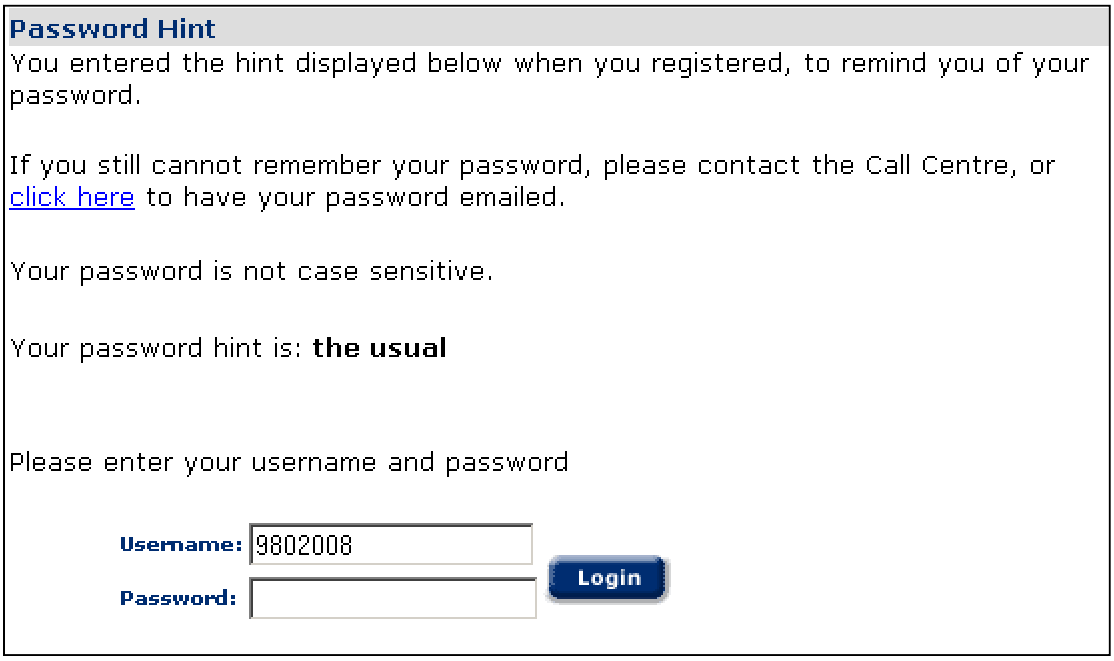
The username you entered does not exist in our records.

You need to enter the username that you chose during registration.

If you have not yet registered click here to register now, else continue, and try to log in again.

Fig 9.27 Incorrect username

Figure 9.28 shows the error message which is displayed if a user enters the incorrect password. The user is informed of their password hint and told that passwords are not case-sensitive. The balance between security and usability is once again evident as a password which is case-sensitive is more secure but less usable.



Password Hint

You entered the hint displayed below when you registered, to remind you of your password.

If you still cannot remember your password, please contact the Call Centre, or click here to have your password emailed.

Your password is not case sensitive.

Your password hint is: **the usual**

Please enter your username and password

Username: 9802008

Password:

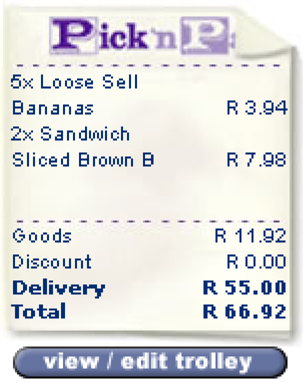
Fig 9.28 Incorrect password

9.9.3 SSL – secure connections

SSL is used during the login and payment procedures, but the user is not informed of this on the login or payment pages. SSL is only briefly mentioned on the help page. In order to be a member of S.A.F.E. a website needs to make use of encryption techniques during transactions. This important point, which could have fostered additional trust, is not conveyed to the user.

9.9.4 Shopping cart and checkout

Pick 'n Pay's online shopping basket looks like a till slip (figure 9.29). This aids the *Learnability* of the site as a till slip is already familiar to a user. Products selected are shown along with their price, delivery charge and total. The user is able to view and edit their basket. The basket is also called a trolley which further reinforces the match between the real world and online environment.

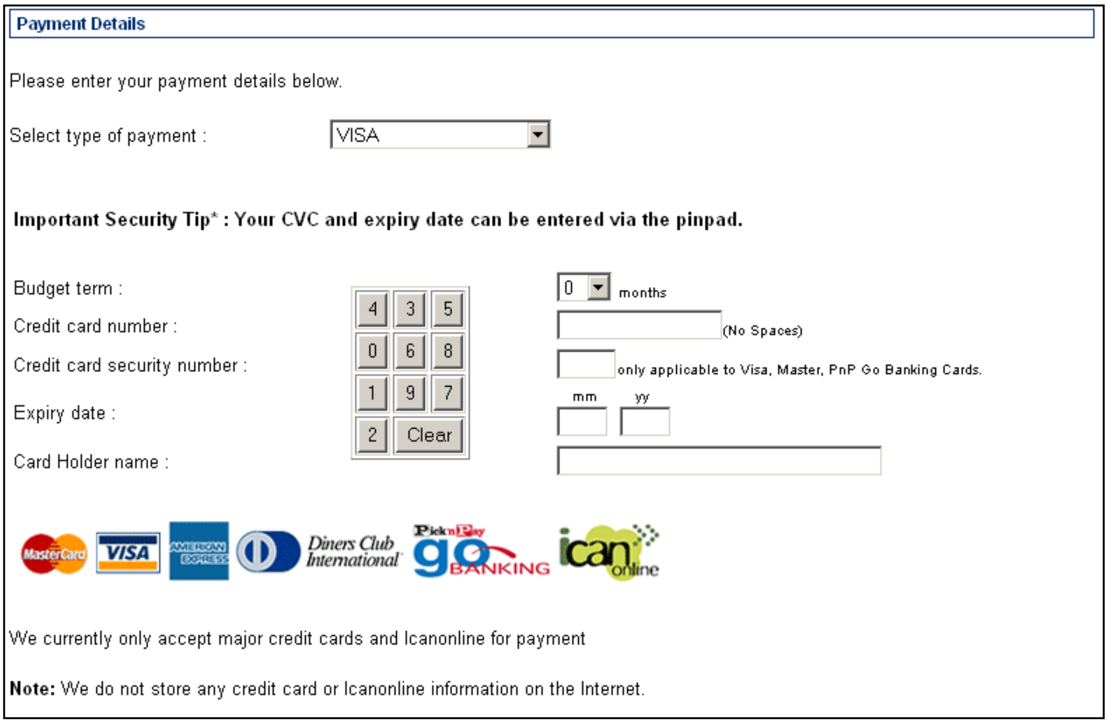


Pick'n Pay

5x Loose Sell	
Bananas	R 3.94
2x Sandwich	
Sliced Brown B	R 7.98
Goods	R 11.92
Discount	R 0.00
Delivery	**R 55.00**
Total	**R 66.92**

Fig 9.29 Shopping cart

Once a user has selected their purchases, they can proceed to checkout (figure 9.30).



Payment Details

Please enter your payment details below.

Select type of payment : VISA

Important Security Tip* : Your CVC and expiry date can be entered via the pinpad.

Budget term : 0 months

Credit card number : (No Spaces)

Credit card security number : only applicable to Visa, Master, PnP Go Banking Cards.

Expiry date : mm yy

Card Holder name :

We currently only accept major credit cards and Icanonline for payment

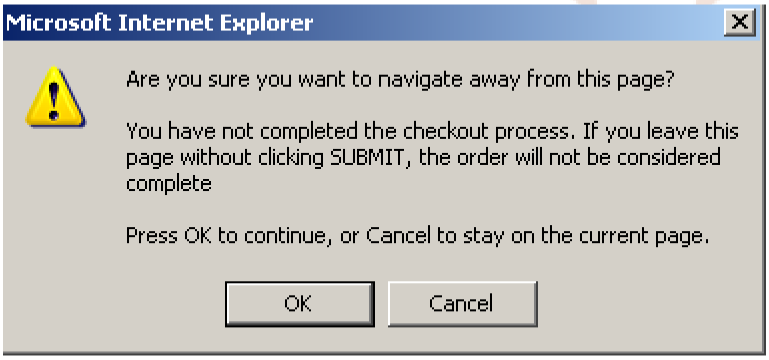
Note: We do not store any credit card or Icanonline information on the Internet.

Fig 9.30 Checkout

On the checkout page (figure 9.30) the user is given various payment options such as a Visa credit card or icanonline direct transfer. As was seen with Kalahari.net, this helps to foster trust as the user is able to choose the payment option with which they feel most comfortable. The user is informed via a 'Security Tip' that they can use the pin pad to enter their credit card and CVC number. However, they are not told why it is important to use the pin pad.

At the bottom of the page the user is given the general assurance 'We do not store any credit card or Icanonline information on the Internet'. This will help to foster a higher level of trust. However, the statement is quite vague and ambiguous. The user might ask questions like 'Then where are my credit card details stored?', or 'Who processes my credit card details?'. A help button is not available on the checkout page.

A 'cancel' button is also not provided on the checkout page. This may cause confusion as the user is not sure what they should do to cancel the transaction. A user who wants to cancel the transaction would have to click the back button on their browser or close their browser. Clicking the back button displays the warning found in figure 9.31.



Microsoft Internet Explorer

Are you sure you want to navigate away from this page?

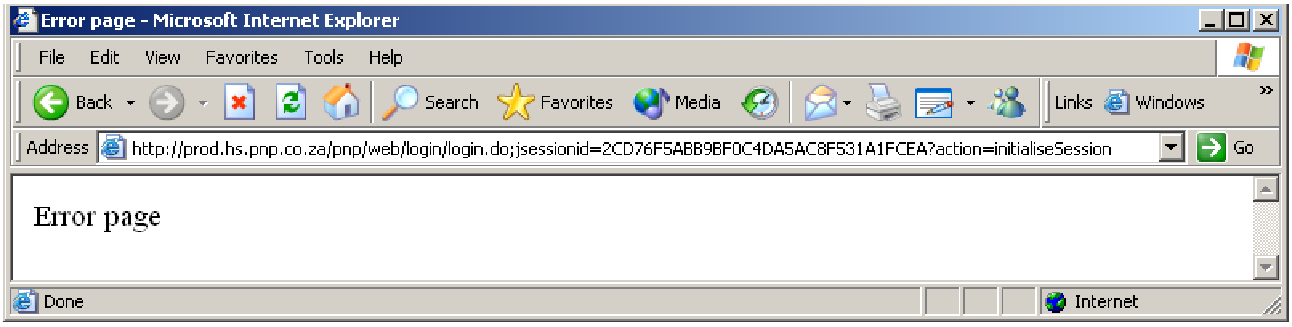
You have not completed the checkout process. If you leave this page without clicking SUBMIT, the order will not be considered complete

Press OK to continue, or Cancel to stay on the current page.

Fig 9.31 Warning message

The logout button, which is present on all the previous Pick 'n Pay pages, is not provided on the checkout page. This means that a user is not able to logout on the checkout page. The absence of cancel and logout buttons may be deliberate. Perhaps Pick 'n Pay is trying to encourage the user to complete their transaction. However, this has a negative effect on the user as they no longer feel in control. The user may feel that they are being 'forced' to complete the transaction.

The message informs the user that their order will not be completed if they use the back button. Using the back button sometimes generates the error message shown in figure 9.32.


Error page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media Links Windows
Address http://prod.hs.pnp.co.za/pnp/web/login/login.do;jsessionid=2CD76F5ABB9BF0C4DA5AC8F531A1FCEA?action=initialiseSession Go
Done Internet

Error page

Fig 9.32 *Error message*

This error page is inadequate as it does not inform the user what the error is, how to fix it and where to get additional assistance.

9.9.5 Logout button

Pick 'n Pay home shopping has a small logout button at the top of the page. It is between a number of other links and is not in a prominent position. Many users may not notice it. While shopping online the user is not encouraged to log off.

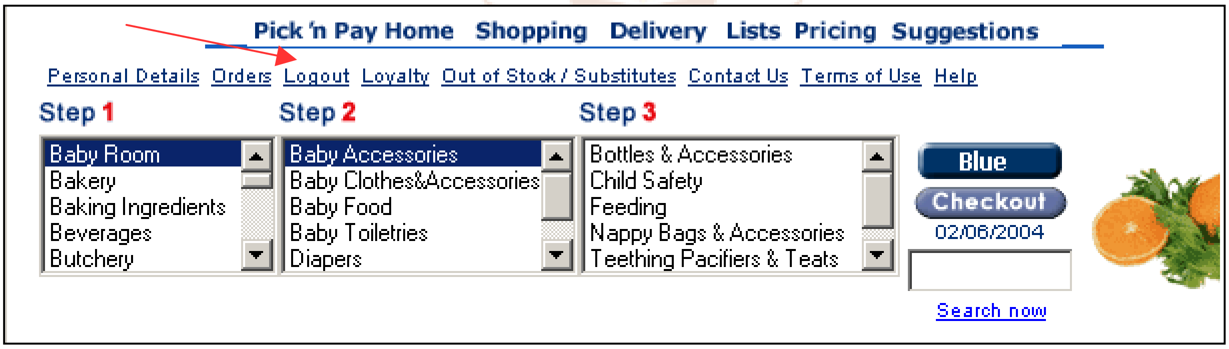
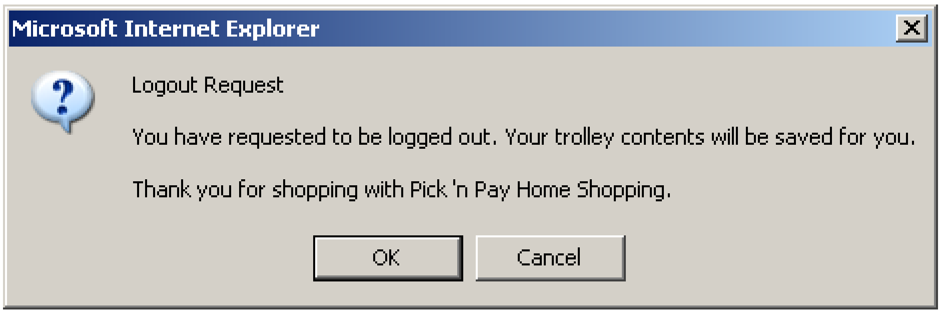


Fig 9.33 *Logout link*

When a user clicks the logout button they are informed that the contents of their trolley have been saved and they are thanked for shopping with Pick 'n Pay (figure 9.34).



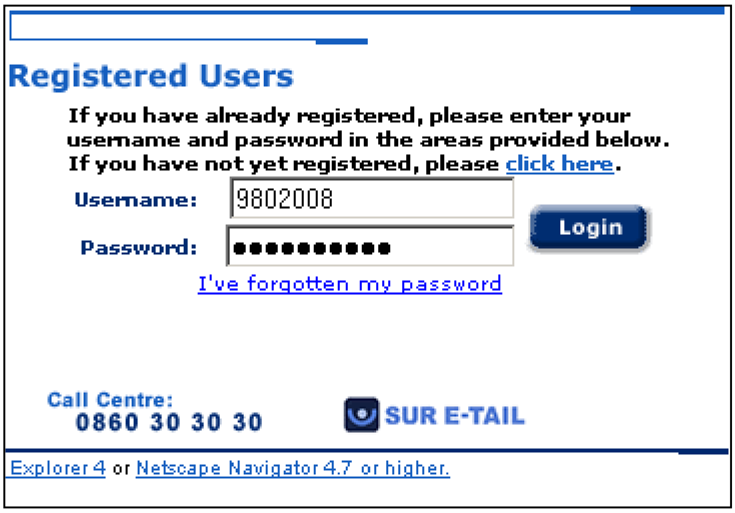
Logout Request

You have requested to be logged out. Your trolley contents will be saved for you.

Thank you for shopping with Pick 'n Pay Home Shopping.

Fig 9.34 *Logout confirmation*

Not using the logout button can have serious implications. If a user does not log out the Pick 'n Pay home shopping's login page remembers the user's password and username (figure 9.35). This potentially allows an unauthorised user access to the previous user's personal details such as name, telephone numbers, ID number, birth date, mother's maiden name and address.



Registered Users

If you have already registered, please enter your username and password in the areas provided below.
If you have not yet registered, please click here.

Username: 9802008

Password: ●●●●●●●●●●●

I've forgotten my password

Call Centre:
0860 30 30 30

Explorer 4 or Netscape Navigator 4.7 or higher.

Fig 9.35 Login – password is remembered

9.9.6 Online help

Picknpay.co.za provides a comprehensive general online help facility which incorporates screen grabs. Information is given on topics such as registration, login, how to shop, orders, delivery, policies, technical issues and terms and conditions.

The information provided on security functions is limited, however, and covered by the following three questions along with answers:

1. Is online shopping safe and secure?
2. How does Pick 'n Pay Home Shopping use personal data?
3. How does Pick 'n Pay Home Shopping protect personal details?

The answers to questions 1 and 3 are a brief discussion on SSL. Pick 'n Pay's privacy policy is given as an answer to question 2. Topics such as firewalls, S.A.F.E., pin pad and the importance of logging out are not covered.

9.10 Conclusion of Picknpay.co.za analysis

A summary in the form of a table is given in this section for each component.

9.10.1 Registration

A summary for the registration component is given in the following table:

Table 9.21 Registration

Criteria	***Conclusion***	***Impact***	
Convey features (16.6% weighting)	**Partial** The user is made to read the terms and conditions before registration. However, the privacy policy is not displayed. User is assured of 'safe and secure shopping'.	User may be hesitant to provide personal details.	8.3%
Visibility of system status (16.6% weighting)	**Partial** User's attention is not drawn to the use of SSL.	User may provide incorrect personal details.	8.3%
Learnability (16.6% weighting)	**Partial** User is able to choose their own username. Interface helps the user to quickly enter their address. Substantial guidelines for a password are not given.	User can choose a username they hopefully will not forget. User may choose an insecure password.	8.3%
Aesthetic and minimalist design (16.6% weighting)	**YES** Simple and clean interface.	Form is quick and easy to complete.	16.6%
Errors (16.6% weighting)	**Partial** User is not warned of 'secure and non-secure' error message.	Many users will not understand the security warning and may terminate the transaction.	8.3%
Satisfaction (16.6% weighting)	**Partial** Password is displayed in plain text.	This may aid the user to remember their password, but the user is not expecting their password to be displayed.	8.3%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 58% level of trust has been developed.	**Total**	**58%**

It appears that Pick 'n Pay have decided to make a trade-off between security and usability. The user is not given security information and their password is displayed in plain text. They are also not encouraged to choose a secure password.

9.10.2 Use of passwords/login

A trust level is calculated in the following table for the passwords/login component:

Table 9.22 Passwords/login component

Criteria	***Conclusion***	***Impact***	
Convey features (16.6% weighting)	**Partial** User is not told that the connection is secure. SUR E-TAIL logo is displayed, but it is not explained.	User may not be aware that measures are being taken to ensure the security of their transaction.	8.3%
Visibility of system status (16.6% weighting)	**Partial** Status of SSL is conveyed by the small padlock in Internet Explorer. User's attention is not directly drawn to SSL.	User might not login.	8.3%
Learnability (16.6% weighting)	**YES** User is able to choose their own username. If the user forgets their password, a password hint is displayed.	User will probably not forget their username.	16.6%
Aesthetic and minimalist design (16.6% weighting)	**YES** Page loads quickly and has a simple design.	User will be able to login quickly.	16.6%
Errors (16.6% weighting)	**Partial** As with Kalahari.net, usability of the site is enhanced by informing the user whether their username or their password was entered incorrectly. User is not told what to do if they forget their password.	Site's security is reduced by providing this additional information.	8.3%
Satisfaction (16.6% weighting)	**Partial** User has to phone the call centre to reset their password or to retrieve their username.	User may feel frustrated as they cannot easily reset their password.	8.3%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 66% level of trust has been developed.	**Total**	**66%**

Pick 'n Pay's login page has the potential to score a high level of trust. However, the measures being taken have not been explained adequately.

9.10.3 SSL

The summary for the SSL component is presented in table 9.23.

Table 9.23 SSL component

Criteria	***Conclusion***	***Impact***	
Convey features (33.3% weighting)	**Partial** The use of SSL is only conveyed on the help page. S.A.F.E. logo is displayed but not explained.	User will not realise that Pick 'n Pay home shopping has been endorsed by a third party.	16.6%
Visibility of system status (33.3% weighting)	**Partial** Status of SSL is conveyed by the small padlock in Internet Explorer.	Only users familiar with SSL will notice the use of encryption.	16.6%
Learnability	Not applicable.	Not applicable.	
Aesthetic and minimalist design	Not applicable.	Not applicable.	
Errors	Not applicable.	Not applicable.	
Satisfaction (33.3% weighting)	**Partial** A user who manages to find additional information on S.A.F.E will be satisfied that adequate security measures have been taken by Pick 'n Pay.	Most users will not realise the importance of S.A.F.E., from a security perspective.	16.6%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 50% level of trust has been developed.	**Total**	**50%**

The user will use the site based on Pick 'n Pay's real-world status, not on their implementation of SSL. Pick 'n Pay have not maximised the advantage of the third-party endorsement of S.A.F.E.

9.10.4 Shopping cart and checkout

The summary of the shopping cart/checkout component follows:

Table 9.24 Shopping cart and checkout component

Criteria	***Conclusion***	***Impact***	
Convey features (16.6% weighting)	**Partial** User is not informed that SSL is being used. Reasons for pin pad are not given.	User may not be aware that security measures are being taken to protect their transaction.	8.3%
Visibility of system status (16.6% weighting)	**Partial** Status of SSL is conveyed by the small padlock in Internet Explorer.	User may be hesitant to supply their banking details.	8.3%
Learnability (16.6% weighting)	**YES** Match between system and real world by using the till slip.	First-time online shoppers will find the shopping basket easy to understand.	16.6%
Aesthetic and minimalist design (16.6% weighting)	**YES** Checkout page has a neat and simple layout.	User will find the checkout process quick and easy.	16.6%
Errors	**NO** Error messages are inadequate.	Users will not know what caused the error messages or what to do next.	0%
Satisfaction (16.6% weighting)	**Partial** Cancel and help buttons are not displayed.	User will not know how to cancel a transaction. User will not be able to access the help when they need it.	8.3%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 58% level of trust has been developed.	**Total**	**58%**

Picknpay.co.za scores poorly in the shopping cart and checkout component. The lack of suitable error messages has the potential to seriously impact the level of trust generated. Error messages during a transaction need to be detailed and reassuring.

9.10.5 Logout button

Table 9.25 presents a summary of the logout button component.

Table 9.25 Logout button

Criteria	***Conclusion***	***Impact***	
Convey features (25% weighting)	**NO** Importance of logging out is not conveyed.	Many users will not log out. User's account may be compromised.	0%

Criteria	*Conclusion*	*Impact*	
Visibility of system status (25% weighting)	**Yes** A message is displayed which states that the user has successfully logged out.	User will hopefully continue logging out in the future.	25%
Learnability	Not applicable.	Not applicable.	
Aesthetic and minimalist design (25% weighting)	**Partial** Logout link is small. It is not in a prominent position.	Many users will not see the link.	12.5%
Errors	An environment which generated errors could not be created.		
Satisfaction (25% weighting)	**Partial** If a user is aware of the logout link, they will be told that their shopping basket has been saved. This will add to their online shopping experience.	The user may close the browser instead of logging out.	12.5%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 50% level of trust has been developed.	**Total**	**50%**

Picknpay.co.za scores poorly with regard to the logout button. The main reason for this is that the logout button is too small and not in the expected position (top right). The user is also not told of the importance of logging out.

9.10.6 Online help

A summary of the analysis of the online help component is given in the following table:

Table 9.26   Online help

Criteria	*Conclusion*	*Impact*	
Convey features (25% weighting)	**Partial** SSL is briefly explained. Pin pad, viruses, firewalls and spyware are not discussed, however.	By reading the help page, a user will be made aware that measures are being taken to ensure the security of their transaction.	12.5%
Visibility of system status	Not applicable.	Not applicable.	

Criteria	*Conclusion*	*Impact*	
Learnability (25% weighting)	**YES**	Most users should be able to understand the help component.	25%
Aesthetic and minimalist design (25% weighting)	**YES** Navigation bar is provided.	User should be able to find what they are looking for.	25%
Errors	Not applicable.	Not applicable.	
Satisfaction (25% weighting)	**Partial** Users looking for information on security will be disappointed.	Users will need to look elsewhere for security information.	25%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 75% level of trust has been developed.	**Total**	**75%**

Not enough information is provided in the help on security features and recommended security practices.

Overall Picknpay.co.za scores:

58%	registration
66%	passwords/login
50%	SSL
58%	shopping cart and checkout
50%	logout button
75%	online help

giving an average level of trust of 60%.

A score of 60% represents an average interface from an HCI-S perspective. It is evident that Pick 'n Pay is using their real-world reputation to help foster trust in an online environment. A number of changes to their interface are strongly recommended to improve the level of trust fostered. Suggested modifications to the interface are discussed in the next section.

9.11 Recommendations for Picknpay.co.za

Recommendations are given in this section on how the interface of Picknpay.co.za can be improved.

9.11.1 Recommendations for registration component

Table 9.27 shows the recommendations for the registration component.

Table 9.27 Registration component

Criteria	***Recommendation***	***Conclusion after recommendation***	***Proposed score***
Convey features (16.6% weighting)	Briefly inform the user of Pick 'n Pay's privacy policy on the registration page.	**YES** User will be aware that their personal information is secure.	16.6%
Visibility of system status (16.6% weighting)	Inform the user that all personal information transferred over the Internet is protected by SSL.	**YES** Users will register with confidence.	16.6%
Learnability (16.6% weighting)	Encourage the user to choose a secure password. Show the user an example of a password or pass phrase.	**YES** User will hopefully choose a password that cannot be cracked easily.	16.6%
Errors (16.6% weighting)	Warn the user that 'secure and non-secure' error messages may be displayed. Explain why these messages are displayed.	**YES** User will continue shopping even if messages are displayed.	16.6%
Satisfaction (16.6% weighting)	Warn the user that on the next page their password will be displayed in plain text.	**Partial** Usability of password will be maintained due to password being displayed in plain text.	8.3%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 91% level of trust has been developed.	**Total**	**Proposed: 91%** **Existing: 58%**

The level of trust generated can be substantially increased by making a few minor changes. It is recommended that Picknpay.co.za continue to display the password in plain text as Pick 'n Pay home shopping is used by many shoppers who have never shopped online before.

9.11.2 Recommendations for passwords/login

Recommendations for the passwords/login component follow in table 9.28.

Table 9.28 Passwords/login component

Criteria	***Recommendation***	***Conclusion after recommendation***	***Proposed score***
Convey features (16.6% weighting)	Provide explanation for SUR E-TAIL logo. Provide link to additional information.	**YES** User will be aware that additional measures have been taken to ensure their safety.	16.6%
Visibility of system status (16.6% weighting)	Inform the user of the use of SSL on the login page.	**YES** User will login with confidence.	16.6%
Errors (16.6% weighting)	In order to maintain a balance between security and usability it is recommended that the error messages remain the same.		8.3%
Satisfaction (16.6% weighting)	Provide feature to retrieve a forgotten username.	**YES** User will be able to retrieve their username without phoning the call centre.	16.6
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 91% level of trust has been developed.	**Total**	**Proposed: 91%** **Existing: 66%**

As with Kalahari.net, it is not recommended to aim for a 100% level of trust, as compromising a user's account will not lead to financial loss for the user. Placing the user in control by allowing them to retrieve their password will aid the usability of the site. To retrieve their username the user could be asked for the email address they used when registering.

9.11.3 Recommendations for SSL component

Picknpay.co.za has the potential to score highly in this component because of the third-party endorsement of S.A.FE. A number of minor changes can help foster a higher level of trust.

Table 9.29 SSL component

Criteria	***Recommendation***	***Conclusion after recommendation***	***Proposed score***
Convey features (16.6% weighting)	Draw the user's attention to the use of SSL on the login, registration and checkout pages.	**YES**	16.6%
Visibility of system status (16.6% weighting)	Draw the user's attention to the small padlock. Place the SUR E-TAIL logo on all pages. Provide explanation of SUR E-TAIL.	**YES**	16.6%
Satisfaction (16.6% weighting)	Include an explanation of SUR E-TAIL.	**YES** User will realise that additional measures have been taken to ensure the safety of their transaction.	16.6%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 100% level of trust has been developed.	**Total**	**Proposed: 100%** **Existing: 50%**

The technology is in place to ensure secure transactions. HCI-S principles now need to be implemented to draw the user's attention to these technologies.

9.11.4 Recommendations for shopping cart and checkout component

Table 9.30 Shopping cart and checkout component

Criteria	***Recommendation***	***Conclusion after recommendation***	***Proposed score***
Convey features (16.6% weighting)	Explain the reason for the pin pad.	**YES**	16.6%
Visibility of system status (16.6% weighting)	Display SUR E-TAIL logo on checkout page.	**YES**	16.6%
Errors (16.6% weighting)	Provide user-friendly error messages which describe the problem and possible solutions.	**YES**	16.6%

Criteria	Recommendation	Conclusion after recommendation	Proposed score
Satisfaction (16.6% weighting)	Provide logout and cancel buttons on the checkout page.	**YES** Users will feel in control of the transaction.	16.6%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 100% level of trust has been developed.	**Total**	**Proposed: 100%** **Existing: 58%**

Important changes are required especially to the 'Errors' criterion. Current error messages are inadequate. Improving the HCI-S in the SSL component will assist in raising the level of trust in the shopping cart checkout component. This is because SSL is used throughout the checkout process.

9.11.5 Recommendations for online help component

The existing online help component scores a respectable 75%. This can be increased by providing more up-to-date security information.

Table 9.31 Online help

Criteria	Recommendation	Conclusion after recommendation	Proposed score
Convey features (25% weighting)	Provide information on current security threats such as spyware. Also provide details on the importance of anti-virus software.	**YES** Users will feel confident that Pick 'n Pay are aware of the latest security threats.	25%
Satisfaction	Provide a search facility.	**YES** After reading the help, the user will feel confident about security principles.	25%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 100% level of trust has been developed.	**Total**	**Proposed: 100%** **Existing: 75%**

9.11.6 Recommendations for logout button component

Table 9.32 includes recommendations for the logout button component.

Table 9.32 Logout button

Criteria	***Recommendation***	***Conclusion after recommendation***	***Proposed score***
Convey features (25% weighting)	Encourage user to logout.	**YES**	25%
Aesthetic and minimalist design (25% weighting)	Increase the size of the logout button and place it at top right-hand corner.	**YES**	25%
Satisfaction (25% weighting)		**YES**	25%
Does the interface lead to trust being developed?			
Trust (100% weighting)	A 100% level of trust has been developed.	**Total**	**Proposed: 100%** **Existing: 50%**

Implementing these recommendations will help to ensure that users logout and close a possible security hole.

As can be seen with Kalahari.net, implementing the HCI-S criteria leads to a higher level of trust. Table 9.33 shows that the level of trust between the existing interface and the proposed interface has increased from 61% to 97%.

Table 9.33 Overall score after recommendation

	Existing	***Proposed***
Registration	58%	91%
Passwords/login	66%	91%
SSL	50%	100%
Shopping cart and checkout	58%	100%
Logout button	50%	100%
Online help	75%	100%
Average	**60%**	**97%**

In the next section the elements which form part of each component in an e-commerce environment are identified.

9.12 Reasons why certain e-commerce sites foster a higher level of trust

Table 9.34 shows the comparison between the three e-commerce sites. Scores in blue denote the highest scores attained.

Table 9.34 Comparison of e-commerce sites

	Sterkinekor.co.za	***Kalahari.net***	***Picknpay.co.za***
Registration	N/A	**75**	58
Login/passwords	N/A	**83**	66
SSL	50	**83**	50
Shopping cart and checkout	N/A	**90**	58
Logout button	**N/A**	N/A	50
Online help	12.5	**88**	**75**
Level of trust	**31**	**84**	**60**

From the above table it is evident that Kalahari.net scores the highest in four out of five of the components. Kalahari.net also develops the highest level of trust overall. For each component the elements are identified which, when present, help to foster a high level of trust.

9.12.1 Registration

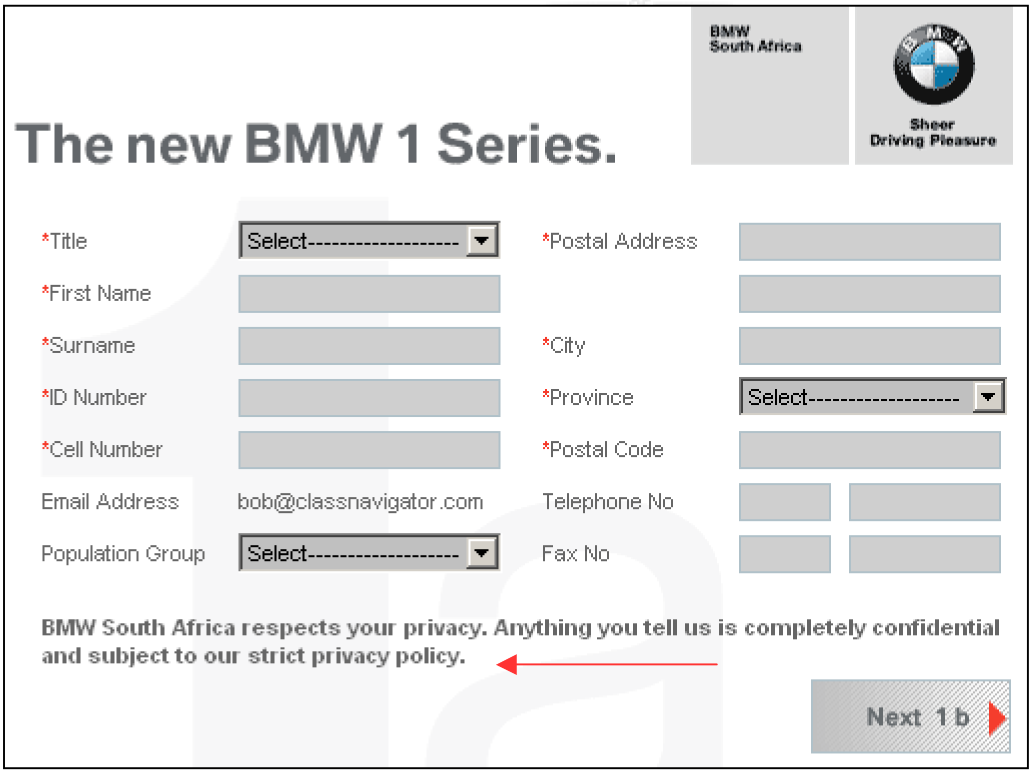
Sterkinekor.co.za does not have a registration component. Kalahari.net and Picknpay.co.za did not score particularly well in this component. This can be seen from table 9.35.

Table 9.35 Registration comparison

	Sterkinekor.co.za	***Kalahari.net***	***Picknpay.co.za***
Inform user of privacy policy	N/A	Provides link to privacy policy	No

	Sterkinekor.co.za	***Kalahari.net***	***Picknpay.co.za***
Encourage the user to choose a secure password	N/A	No	No
Provide user with friendly error messages	N/A	Yes	No
Allow the user to withdraw their personal information	No	No	No

An example of a site which implements some of these elements successfully is www.bmw1series.co.za. This is not an e-commerce site, but it does help to illustrate how the level of trust can be raised by the effective use of a privacy policy. Figure 9.36 shows the registration page. A user is able to register in order to receive information and updates on the new BMW 1 series. A simple reassurance is given to users at the bottom of the page: "BMW South Africa respects your privacy. Anything you tell us is completely confidential and subject to our strict privacy policy." This comment is easy to understand and will help to foster trust. Even though BMW is a well known and trusted brand, an effort has still been made to ensure that this trust is conveyed and extended in an online environment.



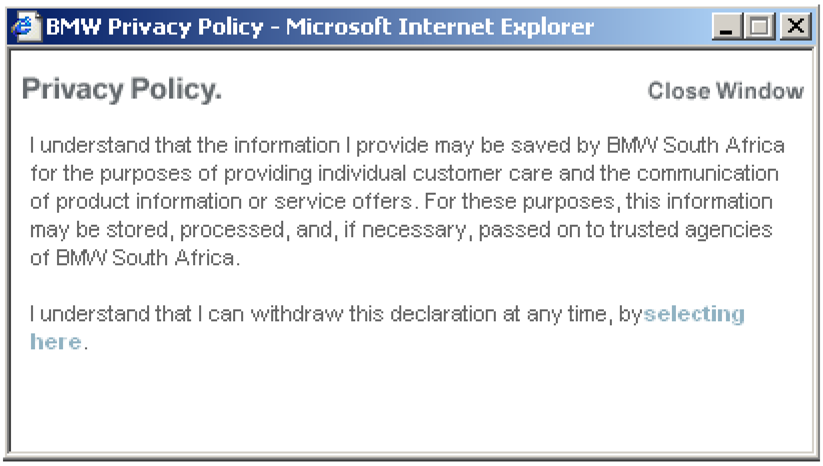
The new BMW 1 Series.

*Title	Select-------------------	*Postal Address	
*First Name			
*Surname		*City	
*ID Number		*Province	Select-------------------
*Cell Number		*Postal Code	
Email Address	bob@classnavigator.com	Telephone No	
Population Group	Select-------------------	Fax No	

BMW South Africa respects your privacy. Anything you tell us is completely confidential and subject to our strict privacy policy.

Fig 9.36 Registration page

BMW's privacy policy is short and easy to understand. It is shown in figure 9.37.



Privacy Policy.

I understand that the information I provide may be saved by BMW South Africa for the purposes of providing individual customer care and the communication of product information or service offers. For these purposes, this information may be stored, processed, and, if necessary, passed on to trusted agencies of BMW South Africa.

I understand that I can withdraw this declaration at any time, byselecting here.

Fig 9.37 BMW privacy policy

The user is also given the option to “withdraw this declaration at any time”. This places the user in control of their personal information.

9.12.2 Login/passwords

The elements which make up a successful HCI-S component for login/passwords in an online shopping environment are different from those found in the online banking environment (section 8.11.1). This is because in an online shopping environment security issues during login have a lower priority than in a banking environment. In an online shopping environment the user can, for example, be allowed to reset their username or password via email, but in a banking environment this would not be acceptable due to the security risks. The table below shows the recommended elements.

Table 9.36 Login/passwords comparison

	Sterkinekor.co.za	***Kalahari.net***	***Picknpay.co.za***
Use third-party endorsements	N/A	Yes	Yes (not explained)
Provide password hints for forgotten passwords	N/A	No	Yes
Allow user to reset their username/password via email/SMS	N/A	Yes	No

Kalahari.net achieved the highest level of trust in this component.

9.12.3 SSL

The elements which make up successful implementation of the SSL component are presented in table 9.37.

Table 9.37 SSL

	Sterkinekor.com	***Kalahari.net***	***Picknpay.co.za***
Inform the user on the home page that they are accessing a secure site	No	Yes	No
Draw the user's attention to the padlock	No	No	No
Use third-party logos for endorsement, e.g. VeriSign	No	Yes	Yes

Sterkinekor.co.za and Picknpay.co.za score poorly in this component. Kalahari.net implements two of the three elements and has the highest level of trust.

9.12.4 Logout button

Only Picknpay.co.za implements a logout button. As was previously mentioned, a logout button for Sterkinekor.co.za is not necessary as users do not need to register. However, it is recommended that Kalahari.net add a logout button.

Table 9.38 Logout button

	Sterkinekor.co.za	***Kalahari.net***	***Picknpay.co.za***
Prominent position (top right)	N/A	N/A	No
Large	N/A	N/A	No
Dedicated logout page informing user of the success of the logout	N/A	N/A	Yes
Explain importance of logging out in help	N/A	N/A	No

Picknpay.co.za only implements one of the elements and scores poorly in this component. Figure 9.38 shows an example from icanonline.co.za which demonstrates from an HCI-S perspective how the logout button should be implemented. It is in a prominent position (top right) and is not easy to overlook.

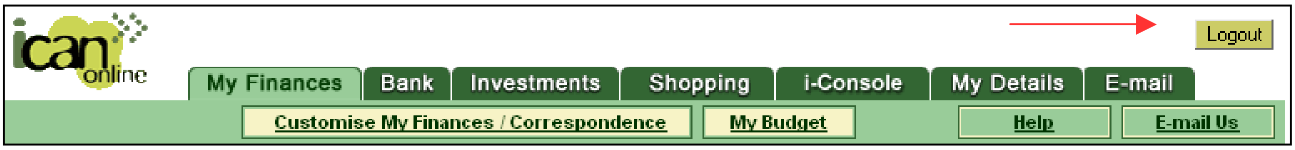


Fig 9.38 Logout button

9.12.5 Online help

The elements which form part of the online help component are the same as those found in the banking environment. Picknpay.co.za and Kalahari.net scored reasonably well in this component. However, the level of trust can be improved by including graphics and additional information on topics such as viruses and firewalls.

Table 9.39 Online help

	Sterkinekor.co.za	***Kalahari.net***	***Picknpay.co.za***
Context-sensitive help	No	Yes	Yes
Use of images and graphics to explain security features	No	No	No
Explain concepts in simple terms	Yes	Yes	Yes
User-friendly navigation	Yes	Yes	Yes
Provide additional help on topics such as viruses, firewalls, spyware and phishing	No	No	No

9.12.6 Shopping cart and checkout help

From an HCI-S perspective, a shopping cart and checkout component will foster a high level of trust if the user is placed in control of the purchasing process. This is evident where three of the four elements for this component relate to placing the user in control. The fourth element is the use of third-party endorsements. Kalahari.net successfully implements all of the elements and scores highly with regard to trust.

Table 9.40 Shopping cart and checkout

	Sterkinekor.co.za	***Kalahari.net***	***Picknpay.co.za***
Use third-party endorsements	N/A	Yes	No
Display prices in shopping cart	N/A	Yes	No
Cancel and back buttons	N/A	Yes	Yes
Offer more than one payment option	N/A	Yes	Yes

9.13 Conclusion

Sterkinekor.co.za, Kalahari.net and Picknpay.co.za were analysed according to the HCI-S criteria, thus meeting the first objective of this chapter. The second objective was then achieved by calculating the level of trust for each interface. Kalahari.net attained the highest score. The elements which make up each component of the interface were also identified. It was found that the presence of certain elements helps the HCI-S criteria to be satisfied, which in turn leads to a higher level of trust, thus meeting the third objective. The aim of this chapter has therefore been met.

This chapter has shown that the HCI-S criteria are valuable in an e-commerce environment. It was also found that the elements which make up a successful component in an e-commerce environment are similar to those found in an online banking environment. However, there are some different elements, particularly in the login/passwords component. This is because more emphasis needs to be placed on security in an online banking environment than in an e-commerce environment.

This chapter has helped to reinforce that HCI-S criteria are generic and can be used to analyse almost any interface which has a security element to it. However, they cannot be blindly applied to an interface without taking the environment into consideration.

The HCI-S criteria have now been used to analyse security interfaces found in different environments. In chapter 5 the first interface, the Windows XP Internet Connection

Firewall, was analysed. The Internet Connection Firewall operates in the traditional standalone software environment. In chapter 8, three banking website interfaces were examined. These banking interfaces form part of the online banking software environment. The third group of interfaces were the e-commerce interfaces analysed in this chapter (chapter 9). The e-commerce sites form part of the online e-commerce software environment. Chapters 5, 8 and 9 form a unit. The purpose of this unit is to demonstrate that the HCI-S criteria are relevant and can be applied in different software environments.

The next chapter in this dissertation is the conclusion.

Chapter 10
Conclusion

In this dissertation the fields of HCI and information security were presented and the common ground between them identified. Various principles were identified in these fields. A model was then developed which helps in the design and analysis of interfaces found in a security environment. This model is in the form of six HCI-S criteria. These HCI-S criteria help programmers to design interfaces which encourage good security principles. It can also be used to analyse existing interfaces. Analysing an interface against the HCI-S criteria outputs a level of trust. Generally the higher the level of trust generated, the better the interface from a security perspective. These criteria are based on existing criteria found in the field of HCI. The criteria were used to analyse interfaces found in the traditional software environment, Internet banking environment and e-commerce environment. Implementing the criteria also helps to generate recommendations on how the interfaces can be made more user-friendly from a security perspective.

The first section of this chapter focuses on the strengths and weaknesses of the set of criteria. This is followed by a discussion on the opportunities for further research in this field. Lastly, some personal comments from the author are presented.

10.1 Evaluation of the criteria

The model that was presented in chapter 4 has both strengths and weaknesses.

10.1.1 Strengths

The advantages of the HCI-S criteria are simple and easy to understand. They are not complicated and should be relatively easy for most programmers and interface designers to implement.

Another advantage is that there are only six criteria. This means that the criteria are easy to remember. A programmer can have them at the back of his mind when designing the interface.

As was seen in the analysis of various interfaces, the HCI-S criteria are flexible and can be used in different environments. Both traditional software interfaces and web interfaces can benefit from the criteria.

The HCI-S criteria are also based on general HCI criteria which are over ten years old. This means that even though the HCI-S criteria are new, they have been built on a tested foundation.

Implementing the HCI-S criteria leads to a higher level of trust. This means that a user is more likely to trust the system and to follow the correct security procedures. The HCI-S criteria can be implemented during the design of an interface or used to analyse an existing interface. Most of the modifications to the interface which the criteria highlight are relatively cheap and easy to implement. The modifications normally only require minor changes to the interface and not huge changes to the code behind the interface. A higher level of trust far outweighs the costs involved in modifying the interface. A substantial increase in the level of security can be achieved with minimal effort.

Implementing the HCI-S criteria also improves the user's experience. This means they are more likely to enjoy using the application. They will also feel more secure and have a higher level of trust in the system.

10.1.2 Weaknesses

The HCI-S criteria also have weaknesses. The criteria are new and have not been tested in all security environments. For example, the HCI-S criteria have not been applied to a security interface found on a PDA.

The criteria are also broad, which means they may not be specific enough for certain situations. A designer may be looking for criteria which are specifically aimed at the interfaces found on ATMs. The HCI-S criteria would be a good starting point but may need to be refined further for ATM interfaces.

The HCI-S criteria are also based on qualitative research, which means it is not based on 'hard facts'. The criteria are open to interpretation and may be implemented incorrectly. The analysis of an interface can also be very subjective with one programmer feeling that the criteria have been met, while another feeling that they have not.

Implementing the HCI-S criteria will lead to an improvement in the level of trust. However, the technology behind the interface may not warrant this level of trust. The HCI-S criteria have created the illusion of a system which should be trusted when the system actually has some technical weaknesses.

10.2 Opportunities for further research

This dissertation has illustrated how important the interface of a security application is. A small change to an interface can have huge repercussions, both positive and negative.

The value of this dissertation is that it is pioneering into the new field of HCI-S. HCI and information security have been well researched, but the field of HCI-S is relatively uncharted. The HCI-S criteria are a starting point for other research in this important field.

The HCI-S criteria need to be applied to a wider range of security interfaces such as cell phone interfaces. The criteria need to be tested to see if they are relevant for all security interfaces or if they need to be modified.

Extensive field research could also be carried out. The purpose of this research would be to identify the correlation between the increase in level of trust and the implementation of good security practices by users. A group of users could be asked to implement a security procedure on an existing interface. The HCI-S criteria could then be applied to the interface and a modified interface developed. A new group of users could then be asked to complete the same security procedure. The findings could then be analysed and the criteria refined as needed.

Additional security interfaces in the security environment could also be analysed. For example, the analysis of a number of anti-virus software interfaces would be valuable.

In chapters 7 and 8 various components were identified which, when present in a web interface, lead to a higher level of trust. The correlation between these components and the HCI-S criteria could be explored further. Perhaps these components could be used alongside the HCI-S criteria to improve interfaces in a web environment.

10.3 Lessons learnt

The author has found the study of information security and interfaces and how the topics relate to each other interesting and beneficial. He has learnt how to analyse objectively and think critically. The author has realised the importance of planning in the design of security interfaces. He has experienced how important the use of established criteria can be in this planning process. The author has seen how important the interface in a security environment is and how small changes to an interface can be hugely advantageous to the user.

In the next section it will be shown how the research goal has been achieved.

10.4 Research goal achieved

In chapter 1 five objectives for this research were set.

The first objective of this research was to determine the current status of HCI within security and to establish if there are adequate criteria that can be used to develop secure HCI. This was achieved in chapters 2 and 3. Chapter 3 provided an overview of HCI in the field of information security. It was illustrated in this chapter how each information security service relates to HCI. In chapter 2 existing HCI criteria developed by Jakob Nielsen were identified as being a suitable base for the further development of HCI-S criteria.

The second objective, to develop formal HCI criteria which are relevant in the fields of security and HCI, was achieved in chapter 4. In chapter 4 the field of HCI-S along with specific HCI-S criteria were introduced.

The third objective of this research was to apply the HCI-S criteria to a security interface found in the traditional software environment. This was achieved by analysing the Internet Connection Firewall in chapter 5. A level of trust was calculated for the interface. In chapter 6 recommendations were made on how the interface can be improved. A proposed interface with these recommendations included was designed and then analysed according to the HCI-S criteria. A new level of trust was then calculated based on the modified interface. It was found that the level of trust in the proposed interface was higher, indicating that the HCI-S criteria can be used to improve the firewall's interface. It was found that the HCI-S criteria are applicable when analysing security interfaces found in a traditional software environment.

The fourth objective was to apply the HCI-S criteria in an Internet banking environment. This was achieved in chapter 8 where three Internet banking sites were analysed. A level of trust was calculated for each interface. Recommendations were then suggested and the proposed interface analysed again. Components were also identified which form part of a successful interface in an online banking environment. With a number of small modifications it was found that the HCI-S criteria are applicable to Internet banking interfaces.

The fifth objective was to apply the HCI-S criteria in an e-commerce environment. Three local e-commerce sites were analysed according to the HCI-S criteria in chapter 9. Modified interfaces, based on the HCI-S criteria, were suggested. The modified interfaces were found to generate a higher level of trust, thus indicating the value of the HCI-S criteria. With a number of minor modifications to the HCI-S criteria, it was found that the criteria are applicable to interfaces found in an e-commerce environment.

The goal of the research, which was to develop criteria which, when applied to an interface, improve the security of a system, has therefore been achieved by meeting the above objectives.

The problem that several interfaces do not encourage users to implement good security habits and principles can therefore be solved by applying the HCI-S criteria.

10.5 Final word

Information security threats in the world continue to grow. New viruses are released on a daily basis and major software companies publish software patches on almost a weekly basis to fix security vulnerabilities in its software. Users' dependence on information technology is also growing at a rapid pace as technology is used to complete more and more tasks. These factors point to the critical importance of information security and the essential need for secure and easy-to-operate computer systems. The researcher believes that HCI-S is one method that can contribute to the development of a safer IT environment for users.

Bibliography

[9DOLL] 9 Dollar Domains (n.d.). *Encryption*. Available from: http://www.9dollardomains.com/encryption.htm (Accessed December 2003).

[ADAM97] Adams, A., Sasse, M. A., Lunt, P. (1997). *Making passwords secure and usable*. Article found in H. Thimbleby, B. O'Conaill & P. Thomas (eds.), People & Computers XII (proceedings of HCI'97) (pg 1-19).

[ADAM99] Adams, A., Sasse, M. A. (1999). *The user is not the enemy*. Found in Communications of ACM. (pg 41-46).

[ALAN98] Dix, A., Finlay, J., Abowd, G. & Beale, R. (1998). *Human Computer Interaction*, 2nd Edition. Europe: Prentice Hall Europe (pg 2-3, 18-19, 162-173, 404-415).

[AMAZ] Amazon.com (n.d.). Available from: http://www.amazon.com/exec/obidos/flex-sign-in/ref=pd_nfyhl_gw_si/102-5862902-9089761?opt=a&page=misc/login/flex-sign-in-secure.html&response=tg/new-for-you/new-for-you/-/main (Accessed July 2003).

[ANSI04] American National Standards Institute (n.d.). Available from: http://www.ansi.org/ (Accessed June 2004).

[ANS01] American National Standard for Telecommunications (2000). Available from: http://www.atis.org/tg2k/_information_security.html (Accessed March 2004).

[ANS01a] American National Standard for Telecommunications (2000). Available from: http://www.atis.org/tg2k/information.html (Accessed March 2004).

[ARRO] Arrow graphics (n.d.). Available from: www.superia.com/ (Accessed August 2003).

[BERN01] Bernard, M. (2001). *Examining user expectations for the location of common e-commerce web objects.* Available from: http://wsupsy.psy.twsu.edu/surl/usabilitynews/41/web_object-ecom.htm or http://psychology.wichita.edu/surl/usabilitynews/41/web_object-ecom.htm (Accessed September 2003).

[BIM00] BIM-TechKnowledge (27 October 2000). *B2C fails to attract South Africans.* Available from: http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905356136&rel=true (Accessed December 2002).

[BORCH01] Brochers, J. (2001). *A Pattern Approach to Interaction Design.* New Jersey: Uni John Wiley and Sons Limited.

[BOTH02] Botha, R. (reinhard@petech.ac.za). (February 2002). RE: Masters research. Principal Lecturer: Business Information Systems, Faculty of Computer Studies, Port Elizabeth Technikon. E-mail to Johnston, J. (johnston@icon.co.za).

[BRINCK02] Brinck, T., Gergle, D., Wood, S. (2002). *Usability for the Web.* San Francisco: Morgan Kaufmann Publishers (pg 2-3).

[BSI04] British Standards Institution (n.d.). Available from: http://www.bsi-global.com/index.xalter (Accessed June 2004).

[BUIE99] Buie, E. (1999). *HCI standards: A mixed blessing.* Available from: http://www.aesthetic-images.com/ebuie/hci_stds.html (Accessed March 2002).

[BUIE00] Buie, E. (2000). *Favorite usability quotes.* Available from: http://www.aesthetic-images.com/ebuie/usability_sec.html#Quotes (Accessed March 2002).

[BUIE01] Buie, E. (2001). *Standards.* Available from: http://www.aesthetic-images.com/ebuie/stds_examples.html (Accessed March 2002).

[CHAIR04] Acherman, R. (2004). *Chairman's Report 2004.* Available from: http://www.picknpay.co.za/pnp/action/media/downloadFile?media_fileid=792 (Accessed

May 2004).

[CHARL03] Clayton, C. (26 July 2003). Your PC, your responsibility, say banks. *Personal Finance.* Available from: http://www.persfin.co.za/index.php?fArticleId=196530 (Accessed August 2003).

[CHES99] eCommerce Trust Study (1999). Research project by Cheskin Research and Studio Archetype/Sapient. 1999, Available from: http://www.cheskin.com/p/ar.asp?mlid=7&arid=40&art=0 (Accessed February 2004).

[CLARK01] Clarke, R. (2001). *Introduction to information security.* Available from: http://www.anu.edu.au/people/Roger.Clarke/EC/IntroSecy.html (Accessed March 2003).

[CLARK03] Clark III, P. (2003). *Corporate governance: The growing importance of data and network security*. Available from: http://www.surfcontrol.com/general/assets/whitepapers/cropped_whitepaper.pdf (Accessed June 2004).

[CORNE] Cornelius (n.d.). *Wall graphic*. Available from: http://www.lonvig.dk/picassomio-the-wall.jpg (Accessed March 2003).

[DHER00] D'Hertefelt, S. (2000). *Trust and the perception of security*. Available from: http://www.interactionarchitect.com/research/report20000103shd.htm (Accessed May 2002).

[DONA00] Donald, N., Nielsen, J. (2000). *Usability on the web isn't a luxury*. Available from: http://www.informationweek.com/773/web3.htm (Accessed July 2003).

[EBUCKS] First National Bank, eBucks online banking (n.d.). Available from: www.ebucks.co.za (Accessed August 2003).

[ECTACT02] Electronic Communications and Transactions Act (2002). South Africa: Government Gazette. Available from: http://www.gov.za/gazette/acts/2002/a25-02.pdf (Accessed March 2003).

[ELOF02] Eloff, J., Eloff, M. (2002). *Human computer interaction: An information security perspective.* Proceedings of IFIP SEC 2002, Cairo, Egypt.

[EMAIL04] PassMark. (service@largebank.com). (17 March 2004). Re: The "Real" Large Bank. E-mail to Johnston, J. (johnston@icon.co.za).

[EMIR00] Internet Statistics (2000). Available from: http://www.emirates.net.ae/channel/main/netads/why-eimnet@ds.html (Accessed September 2003).

[ENVE] Envelope Graphic (n.d.). Available from: www.motherthyme.com (Accessed July 2003).

[EPAY01] EpayNews (2001). *Statistics for online banking*. Available from: http://www.epaynews.com/statistics/bankstats.html (Accessed March 2002).

[FIRST] FIRST Security Papers (n.d.). Available from: http://www.alw.nih.gov/Security/first-papers.html (Accessed March 2003).

[FIRST02] Online banking web site for First National Bank South Africa (2002). Available from: www.firstonline.co.za (Accessed May 2002).

[GOV1] Usability Basics (n.d.). Available from: http://usability.gov/basics/index.html (Accessed July 2004).

[GREEN03] Greene, C. (16 June 2003). *eBlaster spyware has Achilles heel.* Available from: http://www.theregister.co.uk/content/55/31233.html (Accessed October 2003).

[GROW04] Growth of the Internet (2004). Available from: http://www.internetworldstats.com/emarketing.htm (Accessed June 2004).

[HENN04] Henning, E. (2004). *Finding your way in qualitative research*. South Africa: Van Schaik Publishers 2004 (pg 4-5).

[HEWE96] Hewett, Baecker, Card, Carey, Gasen, Mantei, Perlman, Strong, Verplank. (1996). *ACM SIGCHI curricula for human-computer interaction.* Available from: http://www.acm.org/sigchi/cdg/cdg2.html (Accessed April 2002).

[HUMA03] Articles on usability (2003). Available from: http://www.humanfactors.com/downloads/articles.asp (Accessed March 2004).

[INFO03] Info Please (2003). Available from: http://www.infoplease.com/ipd/A0490788.html (Accessed March 2004).

[INTE01] International standards for HCI and usability (2001). Available from: http://www.usabilitynet.org/resources/references/standards.asp (Accessed March 2002).

[ISF00] The Standard for Information Security (2000). *The Forum's Standard of Good Practice.* http://www.isfsecuritystandard.com/pdf/FSOGP_2000.pdf (Accessed April 2003).

[ISII02] User interface design and usability (2002). Available from: http://www.isii.com/ui_design.html (Accessed July 2004).

[ISIZA00] BS7799 accepted as international information security standard (2000). Available from: http://www.itweb.co.za/sections/business/2000/0009291138.asp (Accessed April 2003).

[ISO] The ISO 1799 directory (n.d.). Available from: http://www.iso-17799.com/ (Accessed April 2003).

[ISO04] ISO Online (n.d.). Available from: http://www.iso.org/iso/en/ISOOnline.openerpage (Accessed July 2004).

[ISO9241] Usability Section (2004). *ISO 9241 (Ergonomic Requirements for Office Work with Visual Display Terminals), Part 11 (Guidance on Usability)*. Available from: http://www.aesthetic-images.com/ebuie/usability_sec.html#WhatAreThey (Accessed April 2002).

[ISO11581] International Standard ISO/IEC 11581-3 (2000). Available from: http://www.dcs.ed.ac.uk/teaching/cs4/www/hci/guidelines/ISO-11581-3.pdf (Accessed July 2004).

[JEND00] Jendricke, U., Gerd, D., Markotten, T. (2000). *Usability meets security – The identity-manager as your personal security assistant for the Internet.* Published paper.

[KALA] Kalahari.net (n.d.). Available from: https://secure.kalahari.net/pipeline/signin.asp?toolbar=mweb (Accessed December 2003).

[KAPIN02] Ka-Ping, Y. (2002). *User interaction design for secure systems.* University of California, Berkeley. Published research. Available from: http://www.sims.berkeley.edu/~ping/sid/ (Accessed April 2003).

[KAROT03] Karat, C., Karat, J. (2003). *The evolution of user-centered focus in the human-computer interaction field*. Available from: http://articles.findarticles.com/p/articles/mi_m0ISJ/is_4_42/ai_111505379 (Accessed July 2004).

[KING03] Threat of Internet security breaches increases as traditional systems become impractical (2003). Available from: http://www.itweb.co.za/sections/internet/2003/0302280809.asp?A=REV&O=F (Accessed April 2003).

[MADDIX90] Maddix, F., Horwood, E. (1990). *Human-computer Interaction Theory and Practice.* Great Britain: Prentice Hall Limited.

[MAIL] Mail graphic (n.d.). Available from: http://www.college.columbia.edu/alumni/graphics/mail.gif (Accessed March 2003).

[MERR03] *Merriam-Webster's Collegiate Dictionary.* (2003). Available from: http://www.merriam-webster.com/ (Accessed April 2003).

[MICH95] Michels, S. (1995). *Human-computer interaction in a computer supported collaborative writing environment.* Available from: http://infolab.kub.nl/pub/theses/w3thesis/Hci/hci.html (Accessed April 2002).

[MICRO01] Internet Connection Firewall overview (2001). Available from: http://www.microsoft.com/technet/prodtechnol/winxppro/plan/icf.mspx (Accessed May 2002).

[MILE04] Miles, M., Huberman, A. (1994). *Qualitative Data Analysis*. London: Sage Publications (pg 40).

[MILL56] Miller, G. (1956). *The magical number seven, plus or minus two: Some limits on our capacity to process information.* Psychological Review (pg 63, pg 81-97).

[MOBBS02] Mobbs, P. (2002). *Introducing information security.* Available from: http://secdocs.net/manual/lp-sec/scb1.html (Accessed February 2003).

[MONK95] Monk, A., Gilbert, N. (1995). *Perspectives on HCI Diverse Approaches.* London: Academic Press Limited.

[NED02] Nedbank online banking (2002). Available from: https://netbank.nedsecure.co.za/ (Accessed November 2002).

[NED202] Nedbank online banking (2002). Available from: http://www.nedbank.co.za/indexIE.asp?page=A9 (Accessed November 2002).

[NED301] Nedbank (2003). *% income statement: Big four banks*. Available from: http://www.nedcor.co.za/financials/2003_interim/incomebig4.asp (Accessed December 2003).

[NET] Nedbank online banking (n.d.). Available from: https://netbank.nedsecure.co.za/ (Accessed November 2003).

[NIEL90] Nielsen, J., Molich, R. (1990). *Heuristic evaluation of user interfaces.* Proc. ACM CHI'90 Conference, Seattle, WA, 1-5 April 1990 (pg 249-256).

[NIEL94] Nielsen, J. (1994). *Enhancing the explanatory power of usability heuristics.* Proc. ACM CHI'94 Conference, Boston, MA, April 24-28 1994, (pg 152-158).

[NIEL00] Nielsen, J. (2000). *Hard-to-use sites will fail.* Available from: http://www.ireland.com/newspaper/computimes/2000/0110/compu1.htm (Accessed May 2002).

[NIEL01] Nielsen, J. (2000). *Security & human factors*. Available from: http://www.useit.com/alertbox/20001126.html (Accessed October 2003).

[NIEL02] Nielsen, J. (n.d.) *Heuristic list*. Available from: www.useit.com/papers/heuristic/heuristic_list.html (Accessed June 2002).

[NIELSEN] Nielsen, J. (n.d.). *Papers and essays by Jakob Nielsen.* Available from: http://www.useit.com/papers/ (Accessed May 2003).

[NOKIA04] Nokia (n.d.). Available from: http://www.nokia.com (Accessed July 2004).

[NORM01] Norman, D. (2001). *Nielsen Norman Group*. Available from Donals Norman, www.nngroup.com (Accessed December 2003).

[NORM88] Norman, D. (1988). *The Psychology of Everyday Things*. New York: Basic Books (pg 22).

[NORMAN] Norman, D. (n.d.). *Essays.* Available from: http://www.jnd.org/dn.pubs.html (Accessed February 2003).

[NUA02] How many online? (2002). Available from: http://www.nua.ie/surveys/how_many_online/ (Accessed January 2003).

[ONLI02] The Goldstuck Report (2002). *Online retail in South Africa*. Available from: http://www.theworx.biz/retail02.htm (Accessed September 2003).

[OPTA02] Optavia Corporation (2002). *Usability & e-commerce*. Available from: http://optavia.com/u_ecomm.htm (Accessed December 2002).

[OXFO95] *Advanced Learner's Dictionary* (1995). Oxford: Oxford University Press.

[PASS04] PassMark Security (2004). Available from: http://www.passmarksecurity.com/home.html (Accessed February 2004).

[PELTI02] Peltier, R. (2002). *Information Security Policies, Procedure, and Standards.* Florida: Auerbach Publications (pg 96).

[PICK04] Pick 'n Pay Online Shopping (2004). Available from: https://prod.hs.pnp.co.za/pnp/web/main/A3-4-a.jsp (Accessed April 2004).

[POLS04] Polsson, K. (2004). *Chronology of personal computers.* Available from: http://www.islandnet.com/~kpolsson/comphist/ (Accessed July 2004).

[PRIVA03] Privacy Rights (21 July 2003). *Scam alert: Watch out for "phishing" emails attempting to capture your personal information.* Available from: http://www.privacyrights.org/ar/phishing.htm (Accessed March 2004).

[PUZZLE] Puzzle pieces (n.d.). Available from: http://www.sfwmd.gov/org/wrp/intro_puzzle.html (Accessed March 2003).

[QUEST] Question mark (n.d.). Available from: www.headthing.com/headthing.htm (Accessed April 2003).

[RICH03] Richardson, R. (2003). *Computer Crime and Security Survey*. USA: Computer Security Institute.

[RICHAR03] Richardson, R. (2003). *CSI/FBI Computer Crime and Security Survey.* Computer Security Institute (pg 9).

[SAFE] Safe graphic (n.d.). Available from: http://www.clipart.com/en/search/split?AID=10282909&PID=1028713&nvc_cj=1&q=safe (Accessed August 2003).

[SAFE04] Sure e-Tail (2004). Available from: http://www.safeonline.co.za/?Task=system&Depth=1&CategoryID=2286&ParentCategoryID=2286&xLevel=&RootID=2286&HeadingText=SUR+E%2DTAIL (Accessed May 2004).

[SANS04] Standards South Africa (n.d.). Available from http://www.stansa.co.za/ (Accessed June 2004).

[SANS11581] SANS 11581-1 / SABS ISO/IEC 11581-1:2000 - Information technology - User system interfaces and symbols - Icon symbols and functions (2001). Available from: http://www.stansa.co.za/standardsearch2.asp?s_id=10269&s_document_id=SANS%2011581&keywords=&type=AND&status=ST (Accessed May 2004).

[SECT03] Summary of Section 508 Standards (2003). Available from: http://www.section508.gov/index.cfm?FuseAction=Content&ID=11#web (Accessed June 2004).

[SECU02] The topic: HCI and security systems (2002). Available from: http://www.iit.nrc.ca/~patricka/CHI2003/HCISEC/HCISEC-cfp.html (Accessed January 2002).

[SIGCHI02] ACM Special Interest Group on Computer-Human Interaction (2002). Available from: http://www.hcirn.com/res/org/sigchi.php (Accessed March 2003).

[SKARH04] Skårhøj, K. (2004). *TYPO3 Core APIs*. Available from: http://typo3.org/documentation/document-library/doc_core_api/ (Accessed June 2004).

[SKIDM] Skidmore, M. (n.d.). *Why good design matters.* http://www.automationalley.com/pages/ENews_DesignMatters.asp (Accessed April 2003).

[STAND] Standard Bank Internet banking (n.d.). Available from: https://www12.encrypt.standardbank.co.za/ibsa/InternetBanking (Accessed November 2002).

[STER04] Sterkinekor (2004). Available from: http://www.sterkinekor.co.za (Accessed January 2004).

[STEV03] White, S. (19 August 2003). Available from: http://www.myadsl.co.za/ADSL%20Meeting.pdf (Accessed January 2004).

[STRAU04] Strauss, J., Myburgh, C. P. H. (2004). *Study Guide: Research Methodology.* South Africa: Rand Afrikaans University. (pg 10, 13).

[SULL01] Sullivan, T. (2001). *As simple as possible*. Available from: http://www.pantos.org/atw/35504.html (Accessed January 2003).

[SULL02] Sullivan, T. (2002). *As simple as possible*. Available from: http://www.pantos.org/atw/notes (Accessed January 2003).

[SUND03] Sunday Times (27 July 2003). *Two men linked to ABSA hacker case*. Available from: http://www.sundaytimes.co.za/2003/07/27/news/news35.asp (Accessed October 2003).

[SUTCLI95] Sutcliffe, A. (1995). *Human Computer Interface Design*, 2nd Edition. New York: Macmillan Press LTD (pg 14 -15, pg 17).

[SUTH63] Sutherland, I. (1963). *SketchPad: A man-machine graphical communication system* in AFIPS Spring Joint Computer Conference (pg 329-346).

[TIWA99] Tiwana, A. (1999). *Web Security*. Oxford: Butterworth-Heinemann (pg 46-47).

[TOGNA] Tognazzini, B. (n.d.). *Design section.* Available from: http://www.asktog.com/menus/designMenu.html#designPapers (Accessed February 2003).

[TRUST02] Trust Online. Available from: http://www.trustonline.co.za/ (Accessed October 2002).

[USAB02] Usability Engineering Team, Usability Services, NASA (2002). Available from: http://www.grc.nasa.gov/WWW/usability/educationcss.html (Accessed August 2003).

[VERI04] VeriSign seal for approval (2004). https://seal.verisign.com/splash?form_file=fdf/splash.fdf&type=GOLD&sealid=2&dn=WWW.EBUCKS.COM&lang=en (Accessed March 2004).

[VONS97] Von Solms, S., Eloff, J. (1997). *Information security.* South Africa: Department of Computer Science, Rand Afrikaans University (pg 32).

[VONS97a] Von Solms, S., Eloff, J. (1997). *Information security.* South Africa: Department of Computer Science, Rand Afrikaans University (pg 61-62).

[WARW03] Ashford, W. (6 August 2003). *Unhappy ADSL users join forces*. Available from: http://www.itweb.co.za/sections/telecoms/2003/0308061038.asp?O=FPL (Accessed September 2003).

[WEBP] Digital Web Partners (n.d.). *Site usability.* Available from: http://www.digitalwebpartners.com/html/about_site_usability.html (Accessed July 2003).

[WEBS] Web server graphic (n.d.). Available from: http://www.computer-networking-cables.com/images/network.jpg (Accessed April 2003).

[WEBSI03] Windows XP captures one-third of O/S market on the Web (13 May 2003). Available from: http://www.websidestory.com/pressroom/pressreleases.html?id=193&ctl=x08 (Accessed September 2003).

[WEIK61] Wiek, H. (1961). *The ENIAC story*. Available from: http://ftp.arl.mil/~mike/comphist/eniac-story.html. (Accessed July 2004).

[WEIN04] Wiener, E. (29 January 2004). *ABSA, FNB tops in e-banking*. http://m1.mny.co.za/mnfs.nsf/0/C2256ABF003270C8C2256E2A004783A5?OpenDocument (Accessed April 2004).

[WHIT98] Whitten, A., Tygar J. D. (1998). *Usability of security.* Carnegie Mellon University and University of California. Available from: http://reports-archive.adm.cs.cmu.edu/anon/1998/CMU-CS-98-155.pdf. (Accessed March 2002).

[WIKI03] Information (2003). Wikipedia encyclopedia. Available from: http://www.wikipedia.org/wiki/Information (Accessed June 2003).

[WIKI03a] Information Security (2003). Wikipedia encyclopedia. Available from: http://www.wikipedia.org/wiki/Information (Accessed June 2003).

[WONG02] Wong, D. (2002). *Windows ICF: Can't live with it, can't live without it.* Available from: http://www.securityfocus.com/infocus/1620 (Accessed February 2003).

[WORLD92] *The World Book Dictionary.* (1992). Chicago: World Book Inc.

[YAHOO] Yahoo mail (n.d.). Available from: http://mail.yahoo.com (Accessed October 2003).

[YASK] Electronic commerce in detail (n.d.). Available from: http://www.yaskifo.com/us/info_cartebancaire.htm (Accessed February 2003).

[YEE02] Yee, K. (2002). *User interaction design for secure systems.* University of California, Berkeley. Available from: http://www.sims.berkeley.edu/~ping/sid/. (Accessed November 2002).

[YONA02] Hollander, Y. (2002). *Six top security issues for executives.* Available from: www.computerworld.com/securitytopics/security/story/0,10801,77132,00.html (Accessed February 2003).

[ZAKON04] Zakon, H. (2004). *Hobbes' Internet timeline v7.0.* Available from: http://www.zakon.org/robert/internet/timeline/#1990s (Accessed July 2004).

Security and human computer interfaces

J. Johnston [a], *J. H. P. Eloff* [a] *and L. Labuschagne* [b]

[a] *Department of Computer Science,
University of Pretoria,
0002, Pretoria,
South Africa*

[b] *Department of Computer Science,
Rand Afrikaans University,
PO Box 524,
Auckland Park, 2006,
South Africa*

Abstract

Computer users are exposed to technology mainly through user interfaces. Most users' perceptions are based on their experience with these interfaces. HCI (human computer interaction) is concerned with these interfaces and how they can be improved. Considerable research has been conducted and major advances have been made in the area of HCI. Information security is becoming increasingly important and more complex as business is conducted electronically. However, state-of-the-art security-related product development has ignored general aspects of HCI. The objective of this paper is to promote and enable security awareness of end-users in their interaction with computer systems. It thus aims to consolidate and integrate the two fields of information security and HCI. HCI as a research discipline is a well developed field of study, and the authors are of the opinion that the use of security technologies can be significantly enhanced by employing proven HCI concepts in the design of these technologies. In order to achieve this, various criteria for a successful HCI in a security-specific environment will be examined. Part of the Windows XP Internet Connection Firewall will be used as a case study and analysed according to these criteria, and recommendations will be made.

Keywords: HCI, human computer interaction; Information security; Usability; Trust; Firewalls; HCI-S

1 Introduction

Users experience computers and technology through various user interfaces — mobile phone menus; buttons, icons and windows on a computer screen; dials and knobs in cars; and back buttons and hyperlinks on the Internet. These interfaces are designed to aid the users' understanding of and productivity in using technology. For example, a well designed interface assists the user in becoming proficient in the operation of a software program in a shorter time frame. This enables the user to increase his/her efficiency in completing a certain task. The user feels in control and satisfied with the technology. On the other hand, a poorly designed interface can frustrate the user and hinder the successful completion of tasks, resulting in aversion and scepticism towards using the specific technology in the future.

This paper focuses on aspects of human computer interfaces (HCIs) that are relevant in an information security environment. An example of these is the interface of a software product such as an encryption program or a firewall. These programs deal almost exclusively with security functions. Parts of other interfaces are also intertwined with security features, such as the login interface of an Internet banking website.

Computer and information security continues to grow in importance as the world becomes more connected and an increasing amount of business is transacted electronically. According to the Computer Crime and Security Survey [RICH03], the most popular security technologies used by companies are anti-virus software (99% of companies polled use it) and firewalls (98% of companies). As a result of the proliferation of office and home computers, technologies such as anti-virus software and firewalls have now migrated into the realm of the everyday user, who is not a security expert. This means that the roles of interfaces are crucial in technologies such as anti-virus software and firewalls that convey and guide the user through security features. The user

0167-4048/03

experiences security functionality through the interface. The interface informs the user of the security functions that are available and how to use them. A user may not be aware of a security feature or may use it incorrectly. For example, a personal firewall can only protect a user's computer if it is active, and it will only be active if the user knows how to turn it on. The interface needs to ensure that the user is guided so as to minimise the potential for the user to be the 'weakest' link.

When designing an interface, there is a number of well established criteria that can be applied to increase the efficiency of using various technologies. An example of one such criterion is consistency and standards, as defined by Jakob Nielsen and Rolf Molich in 1990 [MOLICH90]. Consistency and standards mean that, in an interface, the words and actions used need to be consistent and have the same meaning throughout the interface. Consider, for example, some of the firewall products available on the market today. It is common for many of these products to use the terms 'firewall' and 'gateway' synonymously, thereby creating confusion for the average end-user.

The objective of this paper is to show how existing and well established HCI criteria can be employed to analyse and improve the security features of an interface. A number of recommendations are proposed for the modification of currently available interfaces with the ultimate aim of enhancing the usage of the security features of these products.

The first section of this paper discusses the field of HCI. This is followed by the introduction of 10 existing HCI criteria. Once a background to HCI has been established, a new term — HCI-S — is defined. The 10 HCI criteria are then modified, condensed and adapted to focus on the security aspect of HCI. These new criteria are referred to as HCI-S criteria. Windows XP's Internet Connection Firewall is analysed according to these HCI-S criteria. Proposals are then made as to how the interface of the Internet Connection Firewall can be improved.

2 What is HCI?

HCI stands for human computer interaction [MICH01]. From a computer science perspective, HCI deals with the interaction between one or more humans and one or more computers. An image which comes to mind is that of a person using a user interface program, e.g. Microsoft Windows on a workstation [HEWE96].

According to Sjoerd Michels [MICH01], HCI can be defined as: "the part of a computer program responsible for establishing the common ground with a particular (i.e. well known) user. His task is accomplished by expanding and maintaining this common ground throughout the interaction process with the application. Whenever possible, direct manipulation of familiar objects should be the leading interaction principle."

This definition mentions the 'direct manipulation of familiar objects'. This is possible if these objects are known from the real world or from other HCIs. A user is more likely to trust an object that is familiar. The definition also hints at the goal of an HCI, which is to facilitate the interaction between the user and computer. A well designed interface contributes to increased productivity and reduced errors [SCHN93]. For this paper, an 'interface' is a web interface or a traditional graphical user interface on a computer. The computer can be defined as a traditional home or office personal computer or any workstation.

The purpose of HCI is to enhance the 'user-friendliness' of a system. This is sometimes wrongfully perceived as opposing the goals of a secure system [BOTH02]. For example, confidentiality of information is desired in a secure system and is accomplished to a certain degree by the use of passwords. Traditional thinking states that the more passwords there are and the more complex the passwords are, the better the security of a system. However, users do not remember a long complex password, which means they will write it down, leading to the potential breakdown of the security of a system. When it comes to usability principles, the fewer the passwords and the simpler the passwords are, the better. This appears to highlight a contradiction between security and usability. A balance needs to be struck where a secure usable password is created.

In the next section, existing HCI criteria will be introduced that can be used to enhance the 'user-friendliness' of a system.

3 Criteria for a successful HCI

In 1983, Apple Computers released the Apple Lisa to the public [MEYE98]. The Lisa was one of the first commercially available computers to have a graphical user interface. The introduction of graphical user interfaces has made the operation of computers much easier and has also led to huge growth in research in the field of HCI. This in turn has led to a number of principles being established [NIEL94, CARR03]. One of the key players in the field of HCI is Jakob Nielsen. He has been involved in HCI and usability for many years and has developed a list of 10 criteria for a successful HCI [NIEL02]. These criteria, listed in Table 1, have been widely accepted.

Given the established nature of these criteria, it is a good starting point to expand and modify the list of criteria so that they are relevant to an HCI in a security environment. In the next section, the process of expanding and modifying the HCI criteria will start with a definition of a security HCI.

4 Definition of a security HCI (HCI-S)

The objective of this paper is to see how the security of a system can be improved by improving the interface. In order to achieve this objective, a new term 'HCI-S' will be introduced.

Table 1 - Criteria for a successful HCI

No.	Criteria	Description
1	Visibility of system status	It is important for the user to be able to observe theinternal state of the system through the HCI. This can be achieved by the system providing correct feedback within a reasonable time.
2	Match between system and the real world	An HCI which uses real-world metaphors is easier tolearn and understand. This will assist a user in figuring out how to successfully perform tasks.
3	User control and freedom	System functions are often chosen by mistake. The user will then need a clearly marked exit path.
4	Consistency and standards	Words, situations and actions need to be consistent and have the same meaning. A list of reserved words can assist in this area.
5	Error prevention	It is obviously best to prevent errors in the first place through careful design. However, errors do occur and they need to be handled in the best possible way.
6	Recognition rather than recall	The user should not have to remember informationfrom one session to another. Rather, the user should be able to 'recognise' what is happening.
7	Flexibility and efficiency of use	The system should be efficient and flexible to use. Productivity should be increased as a user learns a system. The system should not control the user; rather, the user should dictate which events will occur. The system should be suitable for new and power users.
8	Aesthetic and minimalist design	Information which is irrelevant should not be displayed. The user should not be bombarded with information and options.
9	Help users recognise, diagnose and recover from errors	Error messages need to be clear and suggest a solution.
10	Help and documentation	Users tend to turn to help and documentation as a last resort. Help functionality needs to be context-sensitive and easy to search.

A reference to HCI-S has not been found in current literature. Therefore, for this paper, security HCI (HCI-S) can be defined as: "the part of a user interface which is responsible for establishing the common ground between a user

Table 2. Summary of HCI-S criteria.

No.	Criteria	Description
1	Convey features	The interface needs to convey the available security features to the user.
2	Visibility of system status	It is important for the user to be able to observe the security status of the internal operations.
3	Learnability	The interface needs to be as non-threatening and easy to learn as possible.
4	Aesthetic and minimalist design	Only relevant security information should be displayed.
5	Errors	It is important for the error message to be detailed and to state, if necessary, where to obtain help.
6	Satisfaction	Does the interface aid the user in having a satisfactory experience with a system?
	Does the interface lead to trust being developed?	
	Trust	It is essential for the user to trust the system. This is particularly important in a security environment.

and the security features of a system. HCI-S is human computer interaction applied in the area of computer security."

HCI-S deals with how the security features of a graphical user interface can be made as user-friendly and intuitive as possible. The easier a system is to use, the less likely the user will be to make a mistake or to try to bypass the security feature. This adds to the integrity of a system. HCI-S's goal is to improve the interface in order to improve the security. This leads to the system becoming more secure, robust and reliable.

HCI's focus is on making a computer system as easy to use as possible. However, security features are sometimes perceived to make a system more difficult to use. HCI-S addresses this issue and strikes a balance between security and ease of use.

5 Criteria for a successful HCI applied in the area of security

The interface criteria proposed for HCI-S are listed in Table 2.

The reason for these criteria is to assist in the development and design of interfaces used in a security environment. These criteria are based on Nielsen's HCI criteria, found in paragraph 3 [NIEL02]. They have been modified and condensed to address only the essentials in a security environment. Condensing the criteria makes them easier to remember and modifying them is necessary in order to focus on security.

In the next paragraphs each HCI-S criterion is discussed in more detail.

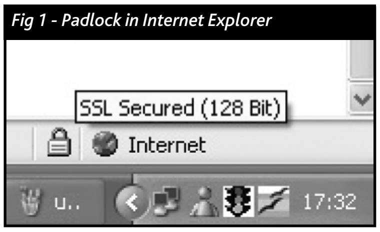
5.1 Visibility of system status

Visibility of system status allows the user to observe the internal state of the system. An example of this is the small 'padlock' which is displayed in the bottom right-hand corner of Internet Explorer when viewing a secure web page (Figure 1). The padlock informs the user of the status of the web page and that encryption is being used.

5.2 Aesthetic and minimalist design

A balance needs to be struck by providing enough information for a first-time user while at the same time not providing too much information for an experienced user. Irrelevant information should not be displayed. The user should not be bombarded with information and options. As far as possible, technical terms should be avoided. For example, if the interface to a security function looks too complicated or confusing, the user may not feel confident enough to use it. By having a minimalist design, this situation can be improved.

Fig 1 - Padlock in Internet Explorer



5.3 Help users recognise, diagnose and recover from errors

Errors which occur when dealing with a security function have the potential to be more lethal than normal errors. For example, take the situation of an error occurring in the middle of a banking transaction and the following error message being displayed: "Your interactive session is no longer active" [FIRST02]. This error message is confusing and may cause a user to feel concerned about the outcome of the transaction. It is important for the error message rather to be detailed and specific, and to state what action needs to be taken and how to obtain additional assistance. A generic message for all errors is not adequate.

5.4 Satisfaction

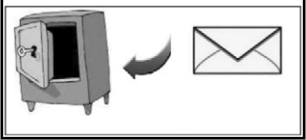
Security is usually not a primary activity for computer users, so their experience with security features needs to be pleasant and satisfying, otherwise they may neglect the security of their system. For example, if it is too much effort for users to encrypt a sensitive document, they may take a chance and email the document unencrypted. Security is also seen by many users as a very technical topic. Techniques such as humour and graphics can be used to introduce important security concepts to users in a more entertaining manner.

5.5 Convey features

The interface should inform the user in a clear manner of the available security features. For example, the security features of integrity and confidentiality are available on most e-commerce web sites. One of the ways in which these features are implemented is through SSL. The use of SSL by a web site should be conveyed to the user by the interface, along with the purpose and benefits of SSL. The use of pictures can be an effective way of conveying features, especially for a user who is not technically minded. Figure 2 shows an example of a graphic which could depict the feature of encryption.

The HCI-S criterion of Convey features informs the user of the available security features, while the criterion of Visibility of system status allows the user to 'see' if these features are active and being used.

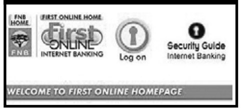
Fig 2 - Encryption



5.6 Learnability

Security is often not a priority for a user, even though it is very important. Therefore it is essential for a security HCI to be as user-friendly and as easy-to-learn as possible. A casual user that has not used the software for a while should not have to learn everything over again [MICH01]. An interface that uses real-world metaphors is easier to learn and understand. For example, items such as keys and locks have real-world uses and meanings. These items and their meanings can be transported and used in an interface. A user that then sees these items will recognise them and have an idea of what they could be used for in the interface. This will assist a user in determining how to perform tasks successfully. An example of this is shown in Figure 3 (the logon keyhole links to the sign-in page).

Fig 3 - Match between system and real world [FIRST02]



An interface that is consistent and based on standards is also easier to learn. Many users are familiar with the conventions of interfaces used in the Microsoft Windows environment. Icons, windows and menus all behave the same in the Windows environment, which means it is easier for a user to learn a new program based on these standards. When it comes to security features in an interface, there are certain conventions which are used frequently, for example usernames and passwords. The user may become confused if different terminology is used, for example 'Profile' instead of 'Username' and 'Access Code' instead of 'Password'. It is therefore advisable for an interface to be consistent and to adhere to standards.

Applying the above six HCI-S criteria in the design of a security feature culminates in establishing trust. Trust is discussed in the next paragraph.

6 The six HCI-S criteria lead to trust

The successful implementation of all the above criteria will lead to trust. Trust is important because if a person is to use a system to its full potential, be it an e-commerce site or a computer program, it is essential for him/her to trust the system.

According to the Oxford English Dictionary, trust can be defined as: "the belief or willingness to believe that one can rely on the goodness, strength, ability of somebody or something" [OXFO95]. This definition can be adapted for the HCI-S criterion of trust to "the belief, or willingness to believe, of a user in the security of a computer system". The degree of trust that users have in a system will determine how they use it. For example, a user that does not trust a web site will not supply his/her credit card details.

The interface plays an important role in fostering trust between the system and user. One way in which this can be done is by the interface informing the user in a clear manner of the risks and how these risks can be minimised. A high-quality interface which projects quality and professionalism will also foster trust. This may, however, be a false sense of trust if the technology behind the interface is not adequate.

As the Internet continues to grow, its success will depend on gaining and maintaining the trust of visitors. Trust on the Internet is not based solely on technical security features, but also on the user's feeling of control of the interactive system [DHER00].

Research performed by InteractionArchitect.com [DHER00] points to six primary factors which convey trust in an e-commerce environment. These factors are fulfilment, technology, seals of approval, presentation, navigation and brand. These factors are important because four of them relate directly to HCI-S:

Fulfilment — This relates to the HCI-S criteria of Convey features and Visibility of system status. The user needs to know which security features are available and be clearly informed when these features are being used. Fulfilment should lead to Satisfaction.

Seals of approval — Seals of approval, for example those used by VeriSign or TRUSTe, need to be in prominent positions. It is also important for their meaning to be conveyed to the user. Seals of approval would come under the HCI-S criterion of Convey features. These seals are third-party endorsements which should help to foster trust between the user and the web site.

Presentation — Aesthetic and minimalist design is important in the presentation of a web site. The result of an aesthetic and minimalist web site is that it is easier to navigate and use than a cluttered web site. This will lead to a more satisfying online experience for the user.

Navigation — An Aesthetic and minimalist design aids navigation. A site which is easy to learn (Learnability) is also easy to navigate.

From the above paragraph it can be seen that these factors overlap with some of the HCI-S criteria. This means that, by applying the HCI-S criteria of Visibility of system status, Satisfaction, Aesthetic and minimalist design, Learnability and Convey features, trust can be developed.

In the next section, the HCI-S criteria will be used to analyse the interface of a firewall. The purpose is to illustrate the application of these criteria.

7 Analysis of Windows XP's Internet Connection Firewall (ICF) according to HCI-S criteria

Microsoft has decided to incorporate a firewall called the Internet Connection Firewall (ICF) in its Windows XP operating system. The ICF comes as standard with both the home and professional versions of Windows XP.

The ICF is aimed at home and small office computer users. Its goal is to provide a baseline intrusion prevention device in Windows XP. The ICF will hopefully protect against scans for information and block unwanted inbound packets [MICRO01]. It is a stateful firewall, which means it only allows incoming packets if they are part of a session originating in the XP computer. Any 'rogue' packets are dropped and optionally logged. The ICF can be activated on any network connection, for example an Internet connection or a local network connection. Microsoft has attempted to make the ICF a simple and unobtrusive security experience.

The reason why the Windows XP ICF has been chosen for analysis in this paper is that, according to WebSideStory, as of May 2003, Windows XP is used by more than a third of all Internet users [WEBSI03]. The next most popular operating system is Windows 98, with a 25% market share [WEBSI03]. This means that there are millions of users around the world that have the ICF installed on their computers. The usability of the interface therefore has the potential to play a huge role in the security of many computers.

In the following paragraphs parts of the ICF interface are analysed according the HCI-S criteria. Recommendations are made on how the interface can be improved according to these criteria.

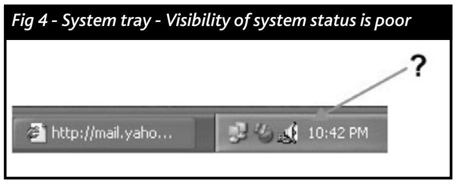
7.1 ICF — Operation

The operation of the ICF is simple. Whenever a network connection, for example a dial-up connection to the Internet, is used, the ICF is active, provided that the ICF option was selected when the network connection was created.

However, many users will not be aware that the ICF is installed and operational because they are not informed of this by the interface. An ICF icon is not displayed in the systems tray and a message does not alert the users to the fact that they are now protected. The Visibility of the system status is therefore not at all clear. The fact that the users are not made aware of the ICF means that they are not encouraged to trust the system.

When a 'rogue' packet is identified by the ICF, it is dropped but the user is not made aware of this. Once again, the Visibility of the system status is poor. The user should be notified of a possible hacking attempt. The user can then decide if he/she wants to ignore any further warnings. The criterion of Satisfaction is not handled well in this case. It could be a very satisfying experience to know that an attempted hack has been thwarted!

Fig 4 - System tray - Visibility of system status is poor



Recommendations for the operation of the ICF

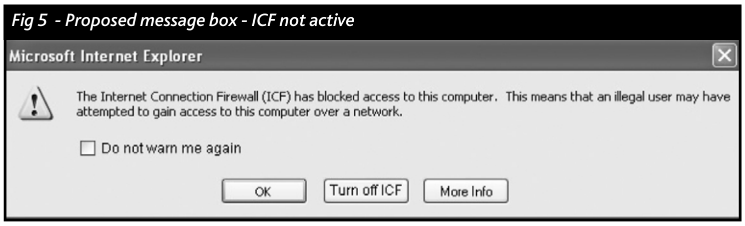
A number of recommendations based on the HCI-S criteria can be made. These recommendations aim at improving the HCI-S of the ICF.

A message box should be displayed as soon as a network connection is used that is not protected by the ICF, warning the user. The message box will aid the Visibility of system status. Figure 5 shows a proposed message box.

An icon should be clearly visible in the system tray whenever the ICF is active, for example an 'F' for firewall (Figure 6).

If the firewall drops packets, the user should be notified via a message box (Figure 7). The user

Fig 5 - Proposed message box - ICF not active


Microsoft Internet Explorer

The Internet Connection Firewall (ICF) has blocked access to this computer. This means that an illegal user may have attempted to gain access to this computer over a network.

☐ Do not warn me again

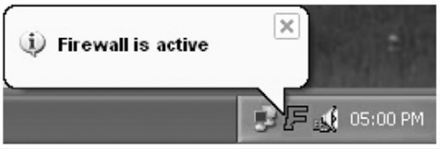
should be able to turn this option on and off. Perhaps the 'F' icon in the system tray could also flash when there is an attempted 'hack'.

7.2 ICF — Configuration

One of the configuration windows of the existing ICF interface is shown in Figure 8. This window has an Aesthetic and minimalist design. The user is not bombarded with options and information.

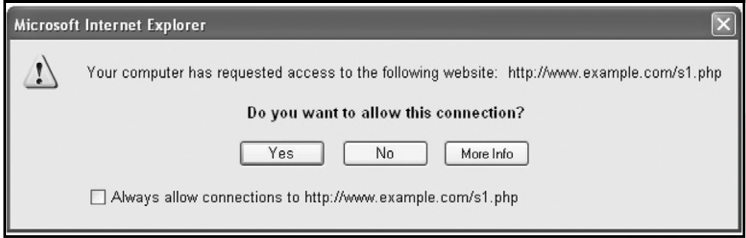
It also has links, such as 'Learn more about Internet Connection Firewall', to more information which should help the user to trust the ICF. The help provides comprehensive information which Conveys the security features. It is easier to trust something that is understood.

Fig 6 - Proposed icon in the system tray



Firewall is active

Fig 7 - Proposed message box - notifies the user that a packet has been dropped



Microsoft Internet Explorer

Your computer has requested access to the following website: http://www.example.com/s1.php

Do you want to allow this connection?

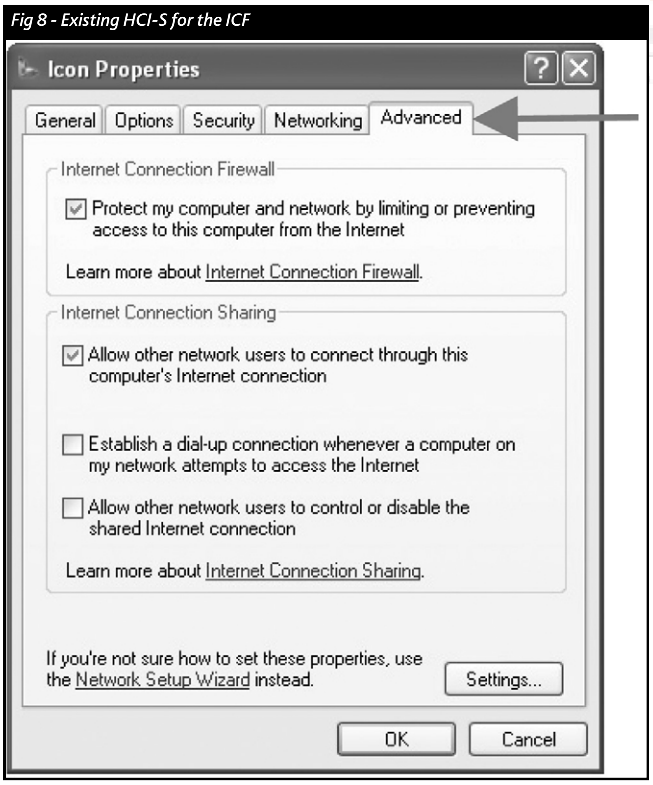
□ Always allow connections to http://www.example.com/s1.php

However, it is not obvious that the 'Settings' button at the bottom of the window is also for the ICF. Clicking this button brings up a window with 'Advanced Settings'. The Advanced Settings window will not be analysed in this paper.

Recommendations for the configuration of the ICF

Figure 9 is a screen shot of the proposed new interface for the ICF. The tab has been changed from 'Advanced' to 'Firewall'. Many users avoid any buttons or tabs with the word 'Advanced' on them. Some users feel that advanced settings should not be changed or explored, as they only need to be used by advanced users that are using their computer for extraordinary tasks. The ICF, however, is not an advanced feature, but rather a standard feature that should be used by all users. The proposed interface is also only focused on the

Fig 8 - Existing HCI-S for the ICF



Icon Properties

Internet Connection Firewall

☑ Protect my computer and network by limiting or preventing access to this computer from the Internet

Learn more about Internet Connection Firewall.

Internet Connection Sharing

☑ Allow other network users to connect through this computer's Internet connection

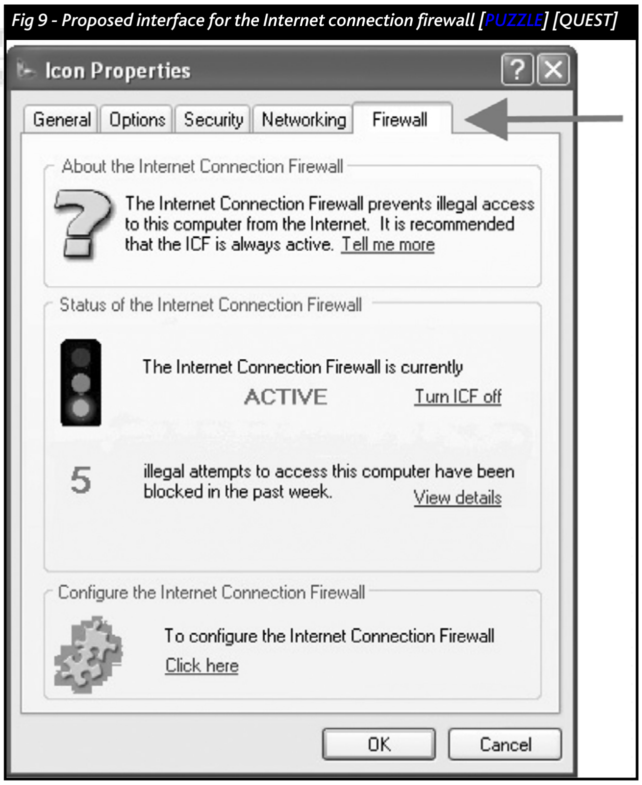
□ Establish a dial-up connection whenever a computer on my network attempts to access the Internet

□ Allow other network users to control or disable the shared Internet connection

Learn more about Internet Connection Sharing.

If you're not sure how to set these properties, use the Network Setup Wizard instead.

Fig 9 - Proposed interface for the Internet connection firewall [PUZZLE] [QUEST]



Icon Properties

About the Internet Connection Firewall

The Internet Connection Firewall prevents illegal access to this computer from the Internet. It is recommended that the ICF is always active. Tell me more

Status of the Internet Connection Firewall

The Internet Connection Firewall is currently ACTIVE Turn ICF off

5 illegal attempts to access this computer have been blocked in the past week. View details

Configure the Internet Connection Firewall

To configure the Internet Connection Firewall Click here

ICF, unlike the existing interface, which also deals with Internet connection sharing (Figure 8).

In order to view the existing interface (Figure 8) of the ICF, the user needs to go through a few steps. For example:

click the 'Start' button;

then click 'Connect to' followed by 'Show all connections';

right click on the Network Connection;

select 'Properties';

then select 'Advanced';

follow this by clicking on 'Settings'.

This process is convoluted and difficult to learn. In order to solve this problem, there are three methods to view the proposed interface (Figure 9) for the ICF:

clicking on the 'F' in the system tray;

selecting the ICF in the Windows Control Panel — this means that a new icon would need to be added to the Windows Control Panel for the ICF;

clicking on the ICF tab when the user is reviewing any network connections, e.g. Internet connections or LAN connections.

These three methods are intuitive and will aid the Learnability of the proposed interface.

The interface in Figure 9 has an Aesthetic and minimalist design. This is evident from the simple layout and the fact that it contains only relevant information for the ICF. It is not complicated and is easy to Learn. This is because the window is based on recognition and not on recall. This means that the user does not need to remember how the ICF works, but rather recognises what the functions do. The Visibility of the system status is clearly displayed by the green 'Active' statement. The user is also informed of any possible hacking attempts. This encourages the user to trust the system. As little technical jargon should be used as possible.

7.3 Summary of analysis of ICF

As has been mentioned, analysis of and recommendations on the entire ICF interface are beyond the scope of this paper. The table below summarises the research findings that have been discussed in this paper, and indicates whether the existing and proposed ICFs meet the criteria.

Table 3. Summary of research findings.

HCI-S Criteria	Existing ICF	Proposed ICF
Convey security features	YES The security features are conveyed by a comprehensive help function.	YES The 'tell me more' links inform the user of the security features.
Visibility of system status	NO It is not obvious whether the ICF is active or working. The user is provided with little feedback.	YES Visibility of system status is clear through the use of an icon in the system tray and via message boxes.
Learnability	NO It is easy for the users to learn how to turn the firewall on and off if they know where to look.	YES ICF is easy to turn on and off. The new interface has the same look and feel as Windows. This means it is easy to learn for someone who is familiar with Windows.
Aesthetic and minimalist design	YES The ICF is unobtrusive and does not annoy the user.	YES The user is only made aware of the ICF when necessary.
Satisfaction	NO Most users will not even be aware that their computers can be protected by the ICF.	YES The inclusion of an icon in the system tray should improve the users' experience and increase their satisfaction.
Do the interfaces lead to trust being developed?		
Trust	NO It is difficult for users to trust something which they are not made aware of.	YES The users are made aware of the firewall and informed of the firewall's actions.

8 Conclusion

The interface of a system is important and cannot be neglected, particularly in a security environment. By applying the HCI-S criteria, a compromise can be reached between the seemingly diverse goals of HCI and security. This will lead to a system which is easier to use and which is more secure.

The Internet Connection Firewall was used as an example of how the HCI-S criteria can be used to improve an interface in a security environment. Only a few simple modifications, some of which have been demonstrated, need to be made which will greatly enhance the users' experience and their computer's security.

The usability of security interfaces is only part of a bigger picture. Even the most user-friendly interface could be avoided by users unless there are policies in place which enforce the use of security programs. For example, a company should have a policy of always encrypting sensitive emails.

This paper showed how the HCI-S criteria can be used to improve the security of a system by modifying the interface. This objective has been accomplished by the discussion on proposals for changing the ICF interface.

The HCI-S criteria can be used by software engineers to ensure that usability is developed into the security interface. The criteria can also be used to evaluate the interfaces of new security products. The criteria will provide direction, from a security point of view, on how an interface can be improved.

References

[BOTH02] Botha, R.A., Principal Lecturer, Business Information Systems, Faculty of Computer Studies, Port Elizabeth Technikon, South Africa. email, February 2002 (reinhard@petech.ac.za)

[CARR03] Carroll, J., (ed), 2003. *HCI Models, Theories, & Frameworks: Toward a Multidisciplinary Science*, Morgan Kaufmann.

[DHER00] D'Hertefelt, S., 3 January 2000. *Trust and the Perception of Security*, http://www.interactionarchitect.com/research/report20000103shd.htm

[FIRST02] Online banking web site for First National Bank South Africa, 2002. http://www.firstonline.co.za

[[HEWE96] Hewett, T.T., Baecker, R., Card, S., Carey, T., Gasen, J., Mantei, M., Perlman, G., Strong, G. and Verplank, W,. 1996. *ACM SIGCHI Curricula for Human-Computer Interaction*. http://www.acm.org/sigchi/cdg/cdg2.html

[MEYE98] Myers, B.A., 1998. A Brief History of Human Computer Interaction Technology, *ACM Interactions*, Vol. 5 (2), March 1998, pp. 44—54.

[MICH01] Michels, S., 1995. *Co-writing, Look and Feel!*, Masters Thesis, http://infolab.kub.nl/pub/theses/w3thesis/Hci/hci.html

[MICRO01] Morgan, D., 2001. Microsoft Corp http://www.microsoft.com/windowsxp/pro/techinfo/planning/firewall/default.asp

[MOLICH90] Nielsen, J. and Molich, R., 1990. Heuristic Evaluation of User Interfaces, *Proc. ACM CHI'90 Conf.* (Seattle, WA, USA, 1—5 April), pp. 249—256.

[NIEL94] Nielsen, J., 1994. *Usability Engineering*, Academic Press Inc

[NIEL00] Nielsen, J., 2000. Hard-to-use sites will fail, *The Irish Times*, January 2000. http://www.ireland.com/newspaper/computimes/2000/0110/compu1.htm

[NIEL02] Nielsen, J., Ten Usability Heuristics, http://www.useit.com/papers/heuristic/heuristic_list.html

[OXFO95] *Oxford Advanced Learner's Dictionary*, 1995. Oxford University Press

[PUZZLE] Puzzle pieces. http://www.sfwmd.gov/org/wrp/intro_puzzle.html

[QUEST] Question Mark. http://www.headthing.com/headthing.htm

[RICH03] Richardson, R., 2003. *2003 CSI/FBI Computer Crime and Security Survey*, Computer Security Institute, www.gocsi.com

[SCHN93] Schneiderman, B., 1993. *Sparks of Innovation in Human-Computer Interaction*, Human-Computer Interaction Laboratory

[WEBSI03] Windows XP Captures One-Third of O/S Market on the Web, 13 May 2003. http://www.websidestory.com/pressroom/pressreleases.html?id=193&ctl=x08x087h27h2