

2016

Identity theft education: Comparison of text-based and game-based learning

Susan Helser
Iowa State University

Follow this and additional works at: <https://lib.dr.iastate.edu/etd>

 Part of the [Engineering Commons](#), [Instructional Media Design Commons](#), and the [Political Science Commons](#)

Recommended Citation

Helser, Susan, "Identity theft education: Comparison of text-based and game-based learning" (2016). *Graduate Theses and Dissertations*. 15930.
<https://lib.dr.iastate.edu/etd/15930>

This Dissertation is brought to you for free and open access by the Iowa State University Capstones, Theses and Dissertations at Iowa State University Digital Repository. It has been accepted for inclusion in Graduate Theses and Dissertations by an authorized administrator of Iowa State University Digital Repository. For more information, please contact digirep@iastate.edu.

Identity theft education: Comparison of text-based and game-based learning

by

Susan Gail Helser

A dissertation submitted to the graduate faculty
in partial fulfillment for the degree of
DOCTOR OF PHILOSOPHY

Major: Electrical and Computer Engineering

Program of Study Committee:
Doug Jacobson, Major Professor
Thomas Daniels
Stephen Gilbert
Jennifer Newman
Steffen Schmidt

Iowa State University

Ames, Iowa

2016

Copyright © Susan Gail Helser, 2016. All rights reserved.

DEDICATION

This dissertation is dedicated to my parents, Claudia A. and David C. Helser. They valued education and the goodness and benefit that it brings. Their love and support made this work possible.

TABLE OF CONTENTS

	Page
DEDICATION.....	ii
LIST OF FIGURES	v
LIST OF TABLES	vi
NOMENCLATURE	vii
ACKNOWLEDGMENTS	viii
ABSTRACT.....	ix
CHAPTER 1 INTRODUCTION: THESIS FORMATTING	10
CHAPTER 2 CHAPTER 2 DESIGNING AND DEVELOPING AN EDUCATIONAL METHOD TO COMBAT IDENTITY THEFT	63
Section I Another Direction.....	63
Section II Games and Educational Games.....	64
Section III Learning Foundations	65
Section IV Assessment	75
Section V Research Design.....	79
Section VI Research Development	85
CHAPTER 3 RESEARCH RESULTS	88
Section I Text-Based and Game-Based Results.....	88
CHAPTER 4 SUMMARY AND CONCLUSIONS	104
Summary.....	104
Conclusions.....	105
REFERENCES	119
APPENDIX A INSTITUTIONAL REVIEW BOARD DOCUMENTS.....	135
APPENDIX B FIGHT IDENTITY THEFT (FIT) INTRODUCTION PANEL	141
APPENDIX C DEMOGRAPHIC INFORMATION	142

APPENDIX D SURVEY 1 AND SURVEY 2 QUESTIONS.....	143
APPENDIX E FIT INFORMATION.....	144
APPENDIX F PARTICIPANT FEEDBACK PANEL.....	153
APPENDIX G FIT SCREEN SHOTS.....	154
APPENDIX H FIT APPLICATION FLOW CHART	161
APPENDIX I FIT SURVEY RESPONSE SCORING SYSTEM	162
APPENDIX J SUMMARY STATISTICS.....	163
APPENDIX K SUMMARY SCORES, TIME, AGE, TECH, EDUCATION	164
APPENDIX L SUMMARY SCORES, TIME, BENEFIT, ENJOYMENT	167
APPENDIX M CHANGE IN PARTICIPANTS' SCORES ON SURVEYS	171
APPENDIX N CALCULATED SCORES, FREQUENCIES AND PERCENTS	174
APPENDIX O GROUPED QUESTIONS RESULTS 127, 368, 459	176
APPENDIX P TEXT AND GAME DATA.....	177

LIST OF FIGURES

	Page
Figure 1 Sample Online Resumes	24
Figure 2 Phishing Activity Trends During Q1: 2016	27
Figure 3 Q 4 2015: Most-Targeted Sectors	29
Figure 4 Port 80 Continues to be the one Most-Targeted for Phishing.....	32
Figure 5 Unique Phishing Sites Detected by Month from January 2015 through March 2016	35
Figure 6 Phishing Reports Received by Month for January 2015 through March 2016	35
Figure 7 Smith and Jones Nevada Licenses	38
Figure 8 Learning Theories and Principles	69
Figure 9 Relationship between Skills and Challenges	74
Figure 10 FIT Screen Shots.....	154
Figure 11 Fight Identity Theft (FIT) Application Flow	161
Figure 12 Frequency Score vs. Benefit	170
Figure 13 Frequency Score vs. Enjoyment	170
Figure 14 Cumulative Score Results for Text-Based and Game-Based Modules	175

LIST OF TABLES

	Page
Table 1 US Sentencing Commission <i>Identity Theft: Final Report</i> , December 15, 1999	39
Table 2 Possible Survey 1 and Survey 2 Responses	95
Table 3 Scoring System to Assess Movement between Survey 1 (S1) and Survey 2 (S2)	161
Table 4 through Table 7 Appendix J	163
Table 8 through Table 17 Appendix K	164
Table 18 through 27 Appendix L.....	167
Table 28 through 37 Appendix M.....	171
Table 38 Appendix N.....	174
Table 39 Appendix O.....	176
Table 40 through 41 Appendix P	177

NOMENCLATURE

gbm	game-based module
tbm	text-based module

ACKNOWLEDGMENTS

I would like to thank my committee chair, Doug Jacobson, and my committee members, Thomas Daniels, Stephen Gilbert, Jennifer Newman, and Steffen Schmidt, for their guidance and support throughout the course of this research.

In addition, I would like to thank my friends, colleagues, the department faculty, and the staff for helping to make my time at Iowa State University a rewarding experience. Also, I would like to express my appreciation to those who were willing to participate in my surveys and observations, without whom, this thesis would not have been possible.

ABSTRACT

Identity theft continues to grow. It drains a host of valuable resources from Society. Trust is affected. *Identity theft* can upend an individual's life and well-being. In the business sector financial losses consume profit and jeopardize the stability of industry. New and complementary approaches to combat the crime are needed.

This research examines two educational methods, one text-based and the other game-based, designed to present information about *identity theft*. For this purpose I developed *Fight Identity Theft* (FIT) software. In addition to collecting demographic information, pre- and post-survey responses and feedback data, FIT provides two educational modules. The program randomly selects the text- or game-based method of delivery. The hypothesis, that game-based learning would be more effective, was confirmed. Participants who received the game-based educational module performed better. Their feedback reflected greater satisfaction with the learning environment. They remained longer in the application.

Digital game-based learning is evolving. Its application to combat *identity theft* can make a difference.

CHAPTER I

INTRODUCTION: THESIS FORMATTING

Section I Overview

The focus of this research is to examine an educational method to mitigate the fast exploding and devastating crime of *identity theft*. The exponentially growing number of victims reflects the artful, deceptive and adaptive nature of the *fraudsters* who commit the crime. The increasing numbers of affected people equate to enormous losses of resources such as time and money. [4] [9] [10] [20] [21] [27] [79] [103] [144] [176]. Ranjit Bose states that, “Identity theft is the fastest growing crime in America; 9.9 million victims were reported last year, according to a Federal Trade Commission survey.” [27]

A myriad of ways exist to perpetrate *identity theft*. Methods range from the uncomplicated to sophisticated, but share one common factor. They can provide the *identity thief* with substantial profit coupled with often little consequence. Detection and prevention strategies have experienced mixed results. *Identity theft* provides challenges for law enforcement and the general public due to the variety of scamming methods in play and use of distributed techniques to launch an attack.

An individual can become a victim of *identity theft* through direct or indirect contact with an *identity thief*. In the case of the former, the attacker perpetrates a *fraud* designed to glean and collect *identity* information from the unknowing person. In the latter case, a victim’s *identity* information is compromised from a third party such as a place of employment, retailer or the government[2] [29] [43] [52] [54] [55] [56] [58] [59] [60] [71] [74] [89] [103] [107] [110] [113] [116] [123] [137] [143] [149] [150] [151] [152] [162]

[163] [168] [169] [170] [171] [172] [173] [174] [179]. The magnitude of the crimes is reflected in these articles. Consider, for example, that in July 2014 the medical community estimated that the number of Americans whose *identities* had been stolen and then used to perpetrate *fraud* in the health industry to be 1.5 million. The average cost per case was determined to be \$20,663. A quick calculation reveals an amount of \$30,994,500,000 [89]. This value is associated with *fraud* only in the medical field. The relative values combined from across various industries place the value of loss in the hundreds of billions of dollars, enough to undermine the economy.

At the personal level following an *identity theft* event, the victim's life is changed forever. The effect can be immediate and cause an individual's world to be flipped on end or can lead to a scenario in which the person continually waits for a "shoe to drop". In either case, there are long-term consequences that affect the victim. Significant resources in the way of time and money are necessary to repair an individual's maligned *identity*. The process is costly [40] [72] [79] [103] [132] [176].

Researchers Shingo Orihara, Yukio Tsuruoka and Kenji Takahashi state, "In the digital world, protecting a user's *identity* is important and ID Theft is becoming a serious social problem, for example, causing an enormous loss in the financial industry. If an attacker steals a user's *identity*, the attacker can easily impersonate the user and do anything as if he/she were the valid user." [124] The White House laid out the very serious issues related to *identity theft* [53] [57]. The Federal Trade Commission (FTC) website for *identity theft* has detailed information about the crime [82].

In order to develop a strategy to help to combat *identity theft*, it is imperative to understand issues related to the crime. To this end, several fundamental areas will be

examined that include a definition of *identity theft*; targets who are vulnerable; methods employed to execute *identity fraud*; and existing countermeasures developed to oppose the crime. After the summary of the introductory issues, detailed information regarding the study follows and includes a description of the design and development of the research to address the problem; analysis and reporting of the results; and concluding remarks.

This paper consists of four chapters. It is structured in the following way. Chapter 1 contains eight sections. Section 1 provides an overview and an introduction of the topic and other related issues. Section 2 discusses definitions of *identity* and *identity theft*. Section 3 explores vulnerable targets and perpetrators of the *fraud*. Section 4 examines causes that support the crime and strategies that are used. Section 5 discusses awareness of the issue. Section 6 reports alarming statistics and economic concerns. Section 7 addresses attempts to fight *identity theft*. Section 8 focuses on the related issues of privacy and security.

Chapter 2 contains two sections. Section 1 discusses the foundations of game-based learning. Section 2 outlines the design and development of the project.

Chapter 3 contains one section that reports the analysis of the study. Text-based and game-based statistics are discussed. Included are results for the three grouped areas under consideration, information regarding responses to individual survey questions, and demographic material and benefit levels measured in the research. Descriptions of the tables listed in the appendices are outlined as well.

Chapter 4 contains one section, the conclusion. Included are a summary of the research findings, suggestions from participants for changes to the application, and a discussion of additional directions to explore. Recommendations from participants and ideas that developed during the study provide opportunities for future work.

References are listed in one section. Appendices consist of A through P. Documents required by the Institutional Review Board (IRB), research results, and other tables are included in the appendix indicated in the body of this work.

Section II Introduction

To better comprehend the consequences of *identity theft*, it is important to first understand the nature of the crime, challenges that it presents, and its affect on society and the individual. A cascade of devastating events can occur as a result of *identity theft*. They can set off a series of crises that embroil the victim in seemingly endless personal and professional turmoil that compromise the individual's credibility. In the end, the major net loss of trust negatively impacts the local and global economies. [3] [28] [29] [65] [92] [105] [110].

As a result of the symbiotic relationship that exists between society and the Internet, we take for granted distributed resources. Education, communication, healthcare, investing, shopping, and the workplace represent a few of the many areas that have been transformed by the expansion of computer networks. Viable authentication is imperative to ensure trust [42] [92] [141]. In order to develop a method to combat *identity theft*, it is important to determine faults in the system that provide attack vectors for *identity thieves* to exploit and to consider people who are at risk of becoming victims [6] [41] [44] [72] [84] [109] [115] [118] [122] [154] [155]. This information will provide the foundation and ground work for later decisions that concern how and where to begin in design and development process of a solution.

Understanding the attacker and contributory factors that promote the crime are essential. *Identity thieves* are creative. They recycle old exploits and continue to develop new ways to bilk victims in order to expand their horizons. A compromised *identity* provides the would-be assailant with all of the benefits and privileges afforded to the actual individual. For example, financial services line of credit or credit options such as student loans, mortgages or credit cards represent abundantly attractive resources to the *identity thief*. Detection and prevention strategies designed to mitigate *identity theft* run the gamut. During the course of this study these methods will be examined to learn which ones represent effective techniques that can be integrated into a solution [19] [22] [23] [27] [39] [40] [61] [62] [67] [85] [86] [87] [88] [103] [111] [112] [117] [121] [124] [130] [132] [136] [161] [176] [183] [187]. A study that focuses on *identity theft* must also consider the ramifications related to issues of privacy versus security [32] [46] [87] [88] [93] [108] [118] [142] [154] [165].

Identity theft is increasing. The Anti-Phishing Working Group reports on the countries hosting the greatest number of *phishing* based *keyloggers* and Trojan *downloaders*. In the 1st Quarter of 2016 the United States ranked number one in the world with 74.54% of these sites [9]. This has been the case for several years. Documentation is available from the Anti-Phishing Working Group (www.apwg.org). According to the same source, the Netherlands has the distinction of being in second place at 2.72% while Canada is in thirteenth place at 0.21%. To understand the magnitude of this problem and to put it into perspective Robert McMillan of the IDG News Service reported on February 21, 2008 in *17 Arrested in Canadian Hack* Quebec provincial police and Royal Canadian Mounted Police forces working in collaboration had broken a major *cybercrime* organization in Canada that

had infected more than 100,000 computers in 100 countries with *botnet phishing* and *spamming* software [106]. The automated programs were used to steal confidential information from users then forward it back to the *botmasters* in Canada. After collecting the information, *identity thieves* then used it for their own nefarious purposes. The removal of a network of this size and the international scope of the crime coupled with the estimated Canadian \$45,000,000 (US \$43,000,000) in damages to computer systems around the world is unprecedented in Canada. Clearly, since Canada's contribution to the worldwide epidemic of identity theft is relatively small, the impact of this crime is significant.

Irrespective of the *identity thief's* main financial objective, the first step that is necessary for any compromise to be of benefit to the *fraudster* is that an individual's *identity* must be stolen. Reasons vary from the direct unauthorized use of the *identity* to perpetrate crime in the victim's name or for use as a quick return commodity to resell for financial gain. An *identity thief* can use a compromised *identity* to mask himself or herself in order to engage in fraud in the victim's name. Once the crime has been committed, the *fraudster* moves on leaving a wake of trouble behind for the unknowing victim to straighten out. If the *identity thief* opts to sell or trade the victim's *identity* information via underground markets, the *fraudster* realizes a direct gain from the transfer of the resource [65].

Identity theft consists of a multifaceted and evolving set of *frauds*. They range in scope from those that are very simple to others that are increasingly complex and sophisticated. Many ruses compromise ordinary systems and structures from routine events. Scamming strategies exploit available resources and often combine the use of technology and *social engineering*. The recognized *fraudsters* turned security specialists Frank Abagnale

and Kevin Mitnick relate numerous methods that incorporate *social engineering* in [3] [4] [109].

Other *identity* related *fraud* attacks are common. A group of *scams* that are easily implemented via the Internet are collectively known as *phishing* [9] [41] [42] [44] [62] [67] [84] [85] [111] [112] [115] [130] [136] [187]. They continue to evolve as well. While Federal guidelines regulate commerce over telephone networks and *fraud* using phone systems is illegal and carries severe penalties, *phone fraud* has increased dramatically and presents a serious threat [128]. It works in much the same way as a *phishing* attack, only rather than the potential victim receiving an email that urges the individual to respond, a direct communication over the telephone is initiated. In some cases an actual human calls the unsuspecting target and attempts to get the person to reveal confidential information, while others are completely automated and begin with a computer that dials phone numbers followed by a sophisticated audio system that sounds like a human being.

The *scam* in the case of *phishing* or *phone fraud* is the same. Specifically, some wonderful or terrible event has occurred that demands the immediate attention of the potential victim. For example, *phishing* attacks can appear to come from an unknown benefactor who requires the victim's bank account information in order to make a generous deposit or seem to be a warning from a known retailer with a message about an account compromise that requires confidential information from the targeted individual. Current *cons* over the telephone include "too good to be true offers" to reduce or eliminate student loan debt, communications from "law enforcement" that claim a complaint that must be addressed immediately has been filed against the person who receives the call, or that Microsoft is

calling to report concerns that the home computer is sending *spam* mail and that it must be stopped. Of course, the caller makes it clear that he or she can assist with these alerts [24].

“Identity theft topped the list of consumer complaints about fraud, according to the U.S. Federal Trade Commission’s annual report for 2005, accounting for 255,000 of the more than 686,000 complaints filed with the agency in 2005 (www.ftc.gov/opa/2006/01/toptenhtm). A prepared statement by the FTC to the U.S. House of Representatives March 30, 2006 ... said *identity theft* victimizes nearly 10 million Americans, with costs to businesses and consumers of almost \$53 billion in 2003, a 79% increase over 2002....” [42]. Prior to moving to the discussion of who is vulnerable, it is important to first define *identity* and *identity theft*.

Section III Identity Defined

The concept of *self* or *identity* represents a basic understanding of who we are across disciplines through our life. *Identity* is a building block and is fundamental factor in our development. Consequential pieces of information and documents such as a social security number or passport provide a person with the means to extend her or his *identity* in a host of directions. This information, unique to a particular individual, is known as *personally identifiable information* or *PII* [70]. Given an established and credible *identity*, an individual can move in a multitude of paths [144]. Everyday people participate in events throughout communities. It is possible to do so, because they have been awarded access or privileges based on their *identity*. A few examples of activities that are possible due to *identity* include securing a job, driving, attending school, donating blood, borrowing books and other materials from a library, acquiring credit to be used for purchases such as home mortgages and other loans, writing checks, travelling to many countries, and pursuing in a wide array of

other interests. An individual establishes and develops an *identity* as a result of the choices and actions he or she makes over time. Community members, friends, and colleagues recognize the individual's physical appearance, voice and behavior. Technical means can be used to validate an *identity* as well. People and technology can be used in combination to vouch for an individual. The one-to-one correspondence of *identity* information with the actual individual that it represents is critical. Once the direct relationship that exists between the person and his or her *identity* information is compromised or broken, lack of trust becomes an issue and can set into motion serious consequences. After an individual learns that his or her *identity* information has been stolen, it is important to take immediate action to help to counter the damage. Multiple researchers have defined *identity* [23] [88] [165].

Identity and *digital identity*, electronically stored data associated with an individual or an organization, are related. An individual's *digital identity* is an extension of the person's *identity*. Information unique to a particular individual that include items such as username and password, biometric data, and unusual or specific attributes are used to authenticate a person on computer networks. The need for viable methods of authentication is growing exponentially due, in part, to the ever greater number of mobile devices and expansion of electronic communication. The consequences of a stolen *digital identity* can be far reaching, long lasting, and devastating. Because of the speed in which electronic data transfer can occur, a compromise requires little time and can go unnoticed until after the event is over and when it is too late to prevent the incident from happening. Digital identity has been defined as the electronic extension of *identity* [14] [88].

Section IV Identity Theft Defined

Deliberate deceptive practices have been in place for ages. The explosion of digital devices has made it possible to conduct technology dependent *fraud* over great distances. *Cybercrime* includes many types of criminal acts that integrate the use of computer systems into scams. In *Cyberethics Morality and Law in Cyberspace, 3rd Ed.* on page 186 Richard Spinello states, “We define *cybercrime* as a special category of criminal acts that is typically executed through the utilization of computer network technologies.” [155] *Fraudsters* who depend on technology based resources to commit crime, exploit the fact that they are able to access desired resources and exit a system quickly. Generally, there exists little personal risk to the attacker. Sometimes the only clue to indicate that a compromise has occurred is a small fragment of computer code that points in the direction of a particular hacker or syndicate.

Heather Morton’s definition of *identity theft* is, “The use of a person's personally identifying information—a name. Social Security number, credit card number or other financial information - without permission, to commit fraud, theft or other crimes.” [112] Fraudulent activity can incorporate the adoption of some other *identity* that is perhaps entirely fictitious or that is associated with another person without the individual’s knowledge. Similar possibilities exist for *fraudsters* to assume and exploit resources granted to other entities such as businesses whether they are fictional or real. While it is often difficult to prosecute, convict and bring those individuals involved in *identity theft* related crimes to justice, accounts exist where disciplinary action was possible [3] [4] [79] [83] [109] [176].

Identity assumption can occur in several ways that include *account take-over* of an actual person's or entity's *identity*, *application fraud* or *true name fraud*, or the complete work-up of a non-existent person for the express purpose to perpetrate *fraud*. The first two are examples of *identity theft*. In the case of *account take-over*, the *thief* assumes the *identity* of the victim to exploit existing resources such as writing checks against the individual's account or using a stolen credit card number to purchase goods in the person's name. In the second case, the *fraudster* uses the victim's *PII* to extend the person's *identity* to acquire resources unknown to the individual such as applying for new credit cards or loans in the individual's name. These methods provide the *identity thief* with access to resources afforded to the victim and do not require the establishment and construction of a completely new *identity*. They represent an advantage to the *fraudster*, because less work is necessary prior to exploitation since the person already exists. It is for this reason that these *frauds* present much greater challenges to law enforcement, since countless legitimate records are associated with the individual. The problem becomes one of determining what *identity* information is true.

The consequences of either offense can be long-term, severe, and can go unnoticed for years. For example, at some future time when an unsuspecting victim attempts to acquire credit in his or her name it may be impossible or exceedingly difficult. If credit can be arranged, interest rates may be extremely high, because of unknown and unpaid bills racked up in the victim's name by the *thief*. The problem for the victim whose *identity* was compromised then becomes one of cleaning up the mess. This involves proving what he or she is responsible for in relation to the numerous unknown events propagated in his or her

name. Numerous detections of *identity theft* exist [10] [27] [103] [137] [144] [183]. Two provided by United States government agencies follow.

The Federal Trade Commission document *Deter, Detect, Defend, Avoid Theft* states, “*Identity theft* is a serious crime. It occurs when your personal information is stolen and used without your knowledge to commit fraud or other crimes. Identity theft can cost you time and money. It can destroy your credit and ruin your good name.” [40] The United States General Accountability Office document *Policy Papers March 2002, Identity theft: Prevalence and Cost Appear to be Growing* indicates on page 48, “... the Secret Service defined ‘*identity theft*’ as any case related to the investigation of false, fraudulent, or counterfeit identification; stolen, counterfeit, or altered checks or Treasury securities; stolen, altered, or counterfeit credit cards; or financial institution fraud.” [79]

Section V Who is Vulnerable?

“Who is at risk of becoming a victim of *identity theft*?” is straightforward, since everyone is a potential target. *Identity thieves* do not discriminate. All genders, age groups, citizens, and non-citizens are possible victims of *identity theft*. Unfortunately, people all too often do not believe that the crime can happen to them. This belief and a lack of awareness of the pervasiveness of *identity theft* are factors that promote the likelihood of becoming a victim. Individuals who are proactive in protecting their *identities* are at risk as well, due to the potential for the compromise of personal data stored on computers [142].

Social engineering is a productive method of securing and exploiting the trust of an unsuspecting target. Its success has been well documented [3] [4] [109]. Also, the ownership of personal information varies greatly and is dependent on the country where it

exists. For example, in some European countries *identity* information strictly belongs to an individual or entity that it relates to in the physical world. Laws protect the person or entity and grant exclusive rights to the *identity* information, regardless of where the information is located or stored. Significant penalties can be levied on offenders. If institutions do not comply with the privacy laws and are determined to be guilty, the judiciary has the ability to punish the responsible parties. A major problem associated with this model is that on average it requires approximately 10 years to enact the necessary legislation in the court system while *identity thieves* continue to move freely and transfer data over the Internet in a few months [154].

In the United States the laws and regulations are entirely different. *PII*, once collected and stored on a computer, becomes the property of the owner of the technology where it is located. At this point, the person who the information initially was related to has no legal claim to it. Conversely, the owner of the technology can use the information in whatever way he, she or it sees fit. For example, *identity* information can be shared over extensive computer networks with parties that the technology owner has a relationship. Also, possible hacking opens the door for the unsuspecting person who provided *PII* to be at risk of *identity theft*. Countless examples of breached computer systems have been reported in government, healthcare and retail disciplines. [64, 65, 66] Because data can be transferred efficiently, it is possible for it to be stolen without the victim's knowledge. In *Markets and Privacy* Kenneth Laudon reports on the establishment of clearing houses for the express purpose to buy, sell and trade bundles of standardized *PII* [93]. In recent U.S. legislation the owner of the technology where *identity* information is stored is accountable. In 1998 *The Identity Theft and Assumption Deterrence Act* was enacted to assist in protecting people from

identity theft [175] [176]. The law was established to punish *thieves* and to hold institutions accountable for failing to prevent data breaches that put individuals at risk of *identity theft*. Subsequent legislation requires that the owner of the technology where the data breach occurred must notify potential victims in writing [70].

Another readily available and significant pool of resources, tailor-made for *identity thieves*, are professionals' vitae posted on the Internet [161]. In order to expedite job-prospects individuals will at times include *PII* in online resumes. Latanya Sweeney researched and reported on this issue [161]. Sweeney collected *PII* during a two year period by using a web-crawler that searched for regular expressions that matched key items such as social security number, date of birth or telephone number. She refers to the information collected in the two consecutive years as DBA and DBB, respectively. A summary of the results of the study is illustrative.

“Of the 150 resumes in the DBA, 140 (or 93%) had complete nine-digit SSNs, whereas 10 had partial, invalid or some other country's number. All of the 75 resumes in DBB had nine-digit SSNs.” [161]

The statistics are troubling and revealing. Sweeney's report included a sample of the information gathered by a web crawler. To protect the individuals' privacy, a number of data items were not revealed in the publication. However, Sweeney noted at the time that the information could be obtained online. The items in Figure 1 appear in Sweeney's article and suggest that the Internet represents a rich space to obtain *PII*. The URLs listed in Sweeney's research are no longer valid. At the time the data was posted on the Internet it was available to the public, so *social engineering* was not required; physical trespassing was unnecessary to

gain access to the *PII*; and hacking of a computer's security features was not needed. In these instances, an *identity thief* was able to view *PII* on the Internet without issue. Sweeney continues work in this area and is an active researcher with a project known as the *Data Privacy Lab*, *SOS Social Security Number Watch* which is a program administered through the IQSS at Harvard University [160].

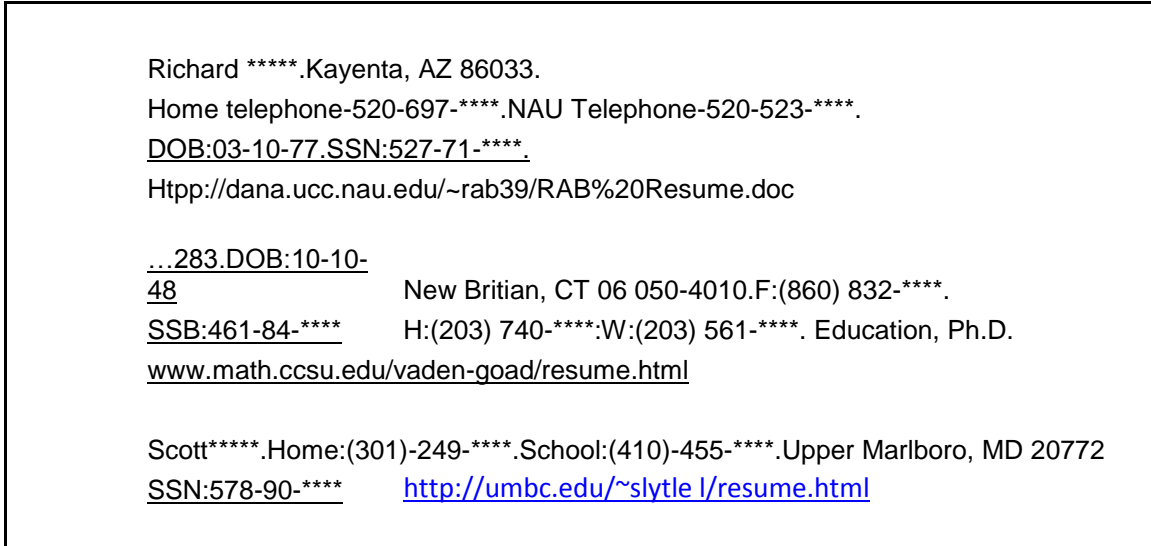


Figure 1: Sample Online Resumes

Young people and adolescents are inclined at times take part in risky behavior often due to a lack of understanding of issues that can affect them. Internet Safety 101 provides information about a variety of technology-based crimes and includes areas that specifically address issues related to young people [82]. Research shows that *PII* that belongs to young adults and adolescents can be obtained in *chat rooms* and on websites [84]. Adults are susceptible to posting *PII* as well. This behavior can be triggered and encouraged by the promise of a free gift such as a cruise, weekend getaway or camera. The ignorance of clear warning signs and the failure to accept the possibility of risk exists. Elderly people tend to accept the written word. Once information enters the home through the Internet via email or

a website application, low cost goods and services appear to be legitimate and are appealing to seniors. Reports reveal that a substantial amount of the population continues to take part in risky choices regardless of age, gender or clear warning signs [106]. Studies show that the same behavior persists in relation to *e-commerce* practices as well with the same result [6] [44] [85] [154].

Prior to discussing who initiates *identity theft*, results compiled from two informal polls of 30 people are instructive. The data provides insight into the need for education about *identity theft*. The first poll was conducted in 2006. The second was taken 10 years later in 2016. Three questions were asked that relate to *identity theft*. The first set of results from 2006 show that individuals in the group did not comprehend the problem.

Q: Have you heard of *identity theft*? A: 10 responded affirmatively

Q: Have you heard of *phishing*? A: 5 responded affirmatively

Q: Have you heard of *LifeLock*? A: 3 responded affirmatively

Ten years later in 2016 a second group of 30 people were asked the same three questions with the results that follow.

Q: Have you heard of *identity theft*? A: 30 responded affirmatively

Q: Have you heard of *phishing*? A: 22 responded affirmatively

Q: Have you heard of *LifeLock*? A: 10 responded affirmatively

The government, the news media, businesses and others have been at work to educate the public about *identity theft*. However, more must be done.

Section VI Who Perpetrates *Identity Theft*

Advances and the reduction in the cost of technology have provided numerous and far-reaching benefits for society. The communication industry has moved from strictly audio

signals to allow for large data sets so that images and video files can be transferred in near real-time. At the same time, developments have made it possible to provide healthcare or financial services to remote locations, this technology has given rise to evolving and costly scams that are more challenging to detect and prevent.

The creativity and motivation of *identity thieves* or *fraudsters* is well-established. Their goal is to acquire *PII* for personal gain by committing a crime in the victim's name or by selling the *identity* information in underground black-market organizations [65]. Research confirms the growing rate of stolen *identity* information. Valid social security numbers have a value of approximately \$25. Other pieces of *identity* information such as date of birth, credit card numbers and medical insurance documentation range in cost and do not exceed \$20. Bank account numbers for accounts with \$70,000 to \$150,000 are worth around \$300. Complete *identity* packets are available for around \$1200 [8] [37] [146] [175].

In the early days of hacking, the perpetrator considered breaching a security system as a form of entertainment or as a "game". Often these individuals were adolescents with an excess of time available to locate weaknesses in security protocols and then figure out ways around them. Accolades received from fellow hackers and boasting rights were their reward. For example, as a result of compromising a computer system teens were able to alter electronically stored records at a school. This type of "chicanery" has been replaced by technology dependent crime such as corporate or international espionage and *identity theft*. The stakes are higher [183].

Phishing and related scams such as *spear phishing* are methods employed to steal *PII* to commit *identity theft* [29] [110] [127] [153]. In the case of *phishing*, these schemes can be understood quite literally as casting out a giant net with the expectation of hauling in a

collection of personal information from unsuspecting victims. The idea is that a percentage of individuals will respond to the bait contained in an email. The con is a popular exploit in the *identity thief's tool-box* and is effective. For example, if 10% of 1000 people are hooked, 100 sets of *identity* information are obtained by the *fraudster*. Profit to the *thief* is considerable and requires little effort or risk. Targeted individuals unknowingly participate by providing *PII*, often through a web-based application that appears to be legitimate, but that is linked to an untrustworthy server. The victim's *PII* is spirited away to a system controlled by an *identity thief* then sold, traded or used by the *fraudster*.

Phishing sites used to promote *identity theft* can exist in any country, because computer networks are an integral component of the *fraud*. The 15 countries hosting the greatest number of *phishing* sites are represented in Figure 2.

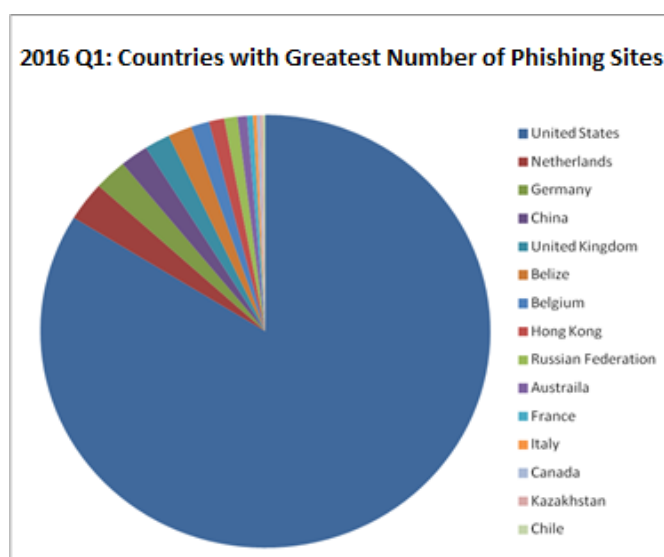


Figure 2: Phishing Activity Trends During Q1: 2016 (APWG - www.antiphishing.org)

The United States continues to hold the “Top Spot” with 77.54%. The values for the remaining countries drop dramatically. Starting with the second highest to lowest the countries include the Netherlands (2.72%), Germany (2.17%), China (1.87%), the United

Kingdom (1.69%), Belize (1.6%), Belgium (1.21%), Hong Kong (1.02%), Russian Federation (0.87%), Australia (0.64%), France (0.39%), Italy (0.25%), Canada (0.21%), Kazakhstan (0.19%), and Chile (0.17%) [9]. The circle graph in Figure 2 represents this information.

According to Sujata Garera, Niels Provos, Monica Chew and Aviel Rubin, *phishing* software is readily available on the Internet. They report that:

“... anyone surfing the web can now get their hands on these kits and launch their own *phishing* attack. These kits are supposed to contain all the graphics, web code and text required to construct bogus web sites designed to have the same look-and-feel as legitimate online banking sites. They also include spamming software which enables potential *fraudsters* to send out hundreds of thousands of *phishing* emails as bait to potential victims. “[67]

Section VII Why Perpetrate *Identity Theft*

Economic gain constitutes the major reason why *fraudsters* engage in *identity theft*. In the report of *Most-Targeted Industry Sectors* in the 4th Quarter of 2015 the APWG lists Retail/Services as the sector as the most desirable target at 42.71%. Financial (18.67%) and Payment (14.74%) Services constitute significant sectors of interest to *identity thieves* as well. The remaining 23.88% is divided between ISPs (12.01%), Multimedia (3.30%), Unclassified (3.13%), Social Networking (2.22%), Government (1.64%), Auction (1.20%), Gaming (0.16%), Classifieds (0.14%), Delivery Services (0.07%) and Education (0.01%) [9]. The circle graph in Figure 3 represents this information. Incurred losses to the individual and business community are overwhelming and threaten to weaken and subvert the world economy [9] [20] [41] [42] [79] [85] [103] [105] [106] [108] [117] [130] [176]

[183]. It is possible for an individual to lose tens of thousands of dollars. At the national level countries such as the United States can sustain losses in the billions of dollars.

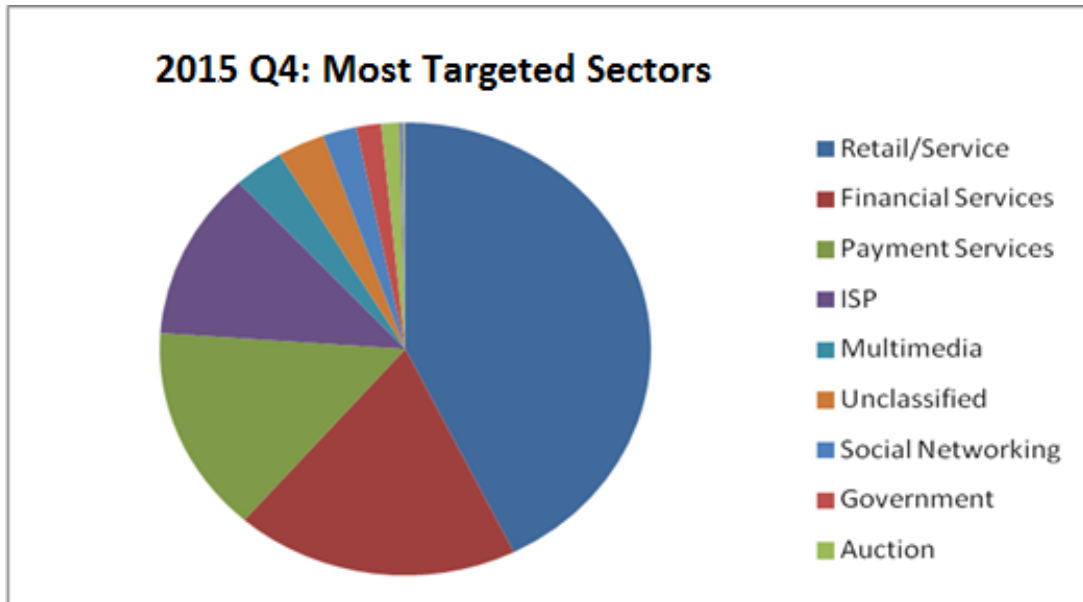


Figure 3: Q 4 2015: Most-Targeted Sectors

The direct financial impact is perilous and contributes to the related and detrimental issue of lack of trust. In turn, credit and the cost of goods are affected. Interest rates and prices for commodities are set at higher levels to cover losses.

Another benefit enjoyed by the *identity thief* that is as valuable as financial reward is the anonymity provided by the use of a victim's *identity*. Crime perpetrated in another individual's name sends law enforcement in the wrong direction. If careful to cover his or her tracks after committing a crime using an assumed *identity*, the *fraudster* can walk away from the event undetected. On the other hand, the unfortunate and often unaware victim is left to deal with cleaning up the mess. To make matters worse, a criminal act can go unnoticed for a significant length of time until the individual whose *identity* was stolen attempts to do to something such as get a prescription filled, apply for a credit card or write a check. The ramifications become apparent when services are withheld or law enforcement

is notified of the whereabouts of the person who is only going about his or her actual business. By this time the *identity thief* has moved on, likely to another assumed *identity*, to commit crime in someone else's name. The person whose *identity* was compromised must prove that he or she did not engage in the unlawful acts. Recovery from these events is costly in terms of time and money.

Frank Abagnale discusses the increase in value of *identities* over time [4]. This is particularly true for young people, adolescents and college students whose ability to acquire credit often grows with their age. For example, hacked university databases provide a plethora of student record information. Consider the potential for committing *fraud* given a host of graduate student records. As professionals in their chosen and respective fields, these individuals will presumably move steadily upward in their careers. As they do so, their salaries and lines of credit increase. For this reason, these *identities* hold significant promise and potential to be used for major gain by an *identity thief*. In this case, rather than selling or trading the stolen *identities* for immediate profit the *fraudster* exhibits restraint with the intention of drawing on the valued resources at some point in the future. Because no clear impact is observed following the compromise, an individual can proceed through life for years prior to the advent of any unusual, unwarranted or unauthorized activity that signals that he or she is a victim of *identity theft*.

Section VIII Assessing Vulnerabilities

Regarding *spam mail* also known as *spam*, the name implies that mail, or rather email, represents an integral component. This is, in fact, the case. The generation of *spam* results in hundreds or perhaps thousands of email messages that can carry an unwholesome

payload. It is highly likely that the true sender opts to conceal his or her *identity*. A variety of methods exist that make it possible to do so such as hijacking a computer connected to the Internet via malware which are programs that consist of harmful computer code designed to benefit the creator and exploit the victim. The infected computer becomes the tool of the *fraudster*. Messages sent from the compromised system retain the host computer's email address and, therefore, do not appear to present a threat to unsuspecting individuals included within the scope of the network associated with the true owner of the infected machine. By obfuscating his or her *identity*, the *fraudster* can present a positive known image that appears to be helpful. The seriousness of this problem cannot be understated. *Spam* represents a direct and substantive challenge, because of the possibility that contains nefarious content as well as the potential impact it can have on system resources. The latter is a known attack, denial of service (DoS) that consumes the band width that is available to address normal activity. It is a highly effective method.

Phishing depends heavily on Internet technologies. The main target of exploitation that hosts web services continues to be Port 80. Figure 4 indicates the relative percent of usage for Port 80 and other ports used to run *phishing* attacks over the Internet.

Other research shows that a significant number of Internet users are ignorant of security features that are in place for their protection [6] [41] [44] [84] [154]. For example, users are unfamiliar with security certificates issued by certificate authorities. Some users who are aware of the existence of security certificates do not know how to check their validity or know the correct location of a lock icon on the web browser. Research shows that a majority of study participants did not understand that the presence of a lock icon in a particular area is for their protection. A related issue is that some users thought that a lock

icon anywhere on the screen indicates a secure site. Another false belief understood by study participants is that if a friend sends a message, then the information is safe to open and to examine.

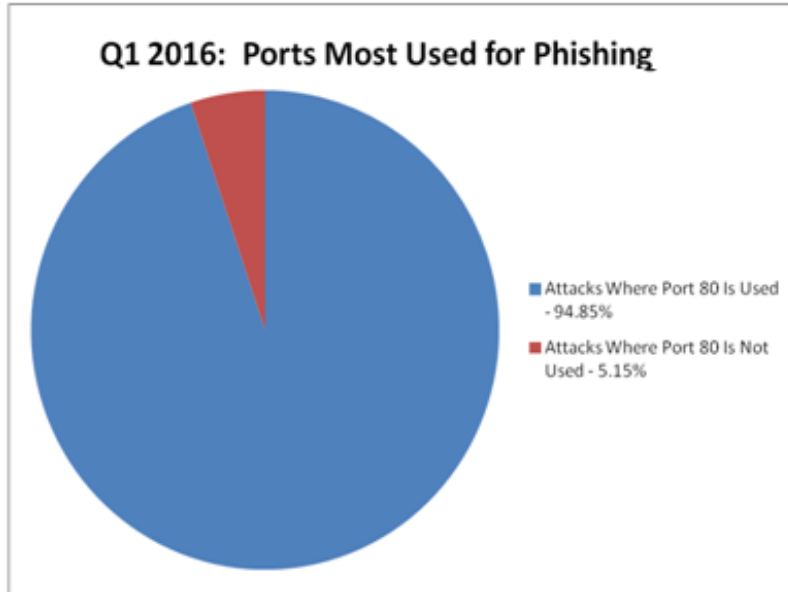


Figure 4: Port 80 Continues to be the one Most-Targeted for *Phishing*

The malleability of *PII* once it is available in electronic form and on Internet represents a serious vulnerability for the victim and great temptation for the *identity thief* [3] [4] [20] [29] [109] [110]. Frank Abagnale discusses his experience with check fraud and related issues of *identity assumption* that are possible, in part, due to the use of digitally stored data [3] [4]. Kevin Mitnick relates similar information [109]. Adrian Cristian Moise examines problems in this area as well [110]. A recent trend reported by Hal Berghel involves documents that he identifies *fungible credentials*. Using these documents the *fraudster* constructs what *appears to be* an authentic *identity* assembled around as little as one bogus piece of identification such as a fraudulently acquired passport. The passport

could be a complete fake or stolen. Items such as these are known as a *breeder documents* which are, in turn, used to attain true identification information [20].

Section IX Strategies Used to Perpetrate Identity Theft

Fraudsters exploit common events to create vulnerabilities inherent within a system. They observe weaknesses or perhaps normal routines that can be modified or manipulated in such a way as to provide a useful and productive advantage. *Spam mail, phishing, social engineering* and *fungible credentials* represent several directions. It is important to understand how the *identity thief* is able to alter trusted activities or items with devastating consequences.

Spam mail or *spam* represents a strategic attack vector for the *fraudster* and can be employed in a host of *scams*. It can be generated by advertisers or other institutions that have no interest in perpetrating *fraud*. However, these sources are responsible for other unfortunate issues unrelated to *identity theft*. In either case, bulk email is sent from a networked device with the intent of reaching as many targets as possible. In the case of *identity theft*, there exists a connection between *spam* and *phishing*. Text-based *phishing* exploits rely on the use of *email* systems. Infected devices can allow the user's address book to be compromised which, in turn, provides access to *email* addresses contained in it. The affected system becomes a tool of the attacker. Depending on the event, the compromise can go unnoticed by the device's owner for a period of time. *Phishing scams* utilize this window of opportunity. *Identity thieves* understand that individuals are more likely to respond to an *email* and provide information to someone they know and trust rather than to an unfamiliar sender. Text included in a *phishing email* appears genuine. Its purpose is to hook the unsuspecting victim. In truth, the *bogus* email contains a hidden and deceptive payload. An

embedded link, invisible to the victim, points to an undisclosed destination and misdirects the user to a path designed to benefit the *fraudster* [65] [84] [111]. Fraudulently sent *phishing* messages deliberately created to look like they come from established financial institutions or retailers and claim to report a problem with the potential victim's account represent examples of frequently used ploys.

Other related *scams* involve a sequence of compromised host devices used in combination to obscure the origin of the attacker. A collection of infected systems behave as a stepping stones and is the source of the name for the *stepping stone attack* [119].

Phishing continues to be a productive method used by *identity thieves*. Numerous resources address *phishing* [9] [41] [42] [44] [61] [62] [65] [67] [84] [85] [115] [111] [130] [136] [187]. In addition to text materials that discuss these issues businesses such as LifeLock (www.lifelock.com) that provide *identity theft* protection, broadcast infomercials and commercials over communication networks. Also, programs that appeal to adolescents such as *The Inspectors* (cbsdreamteam.com/the-inspectors) relate the strategies that are used by *fraudsters* and subsequent problems that can result. More work must be done in this area to inform the public of the relative easy and pervasiveness of *identity theft*. Research indicates that possible victims of *identity theft* constitute a majority. Rachna Dhamija, J.D. Tygar and Marti Hearst discussed findings from their study that examined *phishing* success.

“Good *phishing* websites fooled 90% of participants.

Existing *anti-phishing* browsing cues are ineffective. 23% of participants in our study did not look at the address bar, status bar, or security indicators.

On average, our participant group made mistakes on our test 40% of the time.

Popup warnings about fraudulent certificates were ineffective. 15 out of 22

participants proceeded without hesitation when presented with warnings.

Participants proved vulnerable across the board to *phishing* attacks. In our study, neither [the subject’s] education, age, sex, previous experience, nor hours of computer use showed a statistically significant correlation with vulnerability to *phishing*.” [41]

Figures 5 and 6 show data reported by the Anti-Phishing Working Group. *Phishing* constitutes a major threat and represents a substantial component of Internet-based *fraud* [7] [9] [119]. The number of sites and reports are displayed.

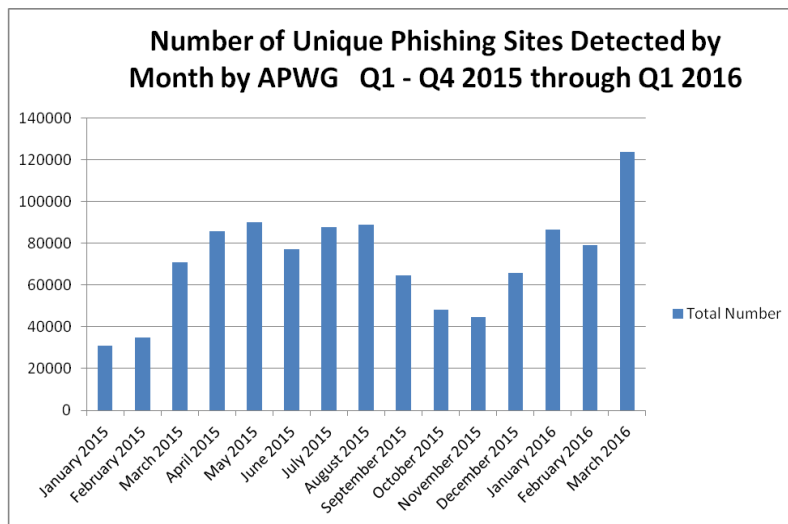


Figure 5: Unique Phishing Sites Detected by Month from January 2015 through March 2016



Figure 6: Phishing Reports Received by Month for January 2015 through March 2016

Social engineering is another method effectively employed by *identity thieves*. The name *social engineering* is descriptive of the events perpetrated by the *thief*. The strategy requires that the *fraudster* gain the trust of the victim or possibly his or her subordinates or colleagues prior to running the *scam*. The *identity thief* performs reconnaissance on the intended victim or perhaps on the “weak links” in the chain. Generally, the ruse develops over a period of time that can span several days or longer. Once the interloper’s work is done gaining trust, conducting the *fraud* is relatively simple, because individuals “on the inside” take part in the process. Pieces of information gathered by *identity thief* can be combined and manipulated so that the *fraudster* is sufficiently cloaked to access the desired resource [4] [10] [14] [29] [109] [110] [118] [144] [155]. This *scam* often depends on the *social engineer* exploiting a victim’s expected behavior or possibly those around him or her. A receptionist, whose job it is to provide service, might be targeted. For example, during a series of what appear to be routine telephone calls a *fraudster* could ask the receptionist to provide details about his or her supervisors’ schedule such as when he or she is unable to take a phone call or meet in person due to prior commitments. The *fraudster* then uses this information to set the *con* at an optimal time, say when the person of interest in a decision-making position is unavailable. Because the *social engineer* has determined usual events that include regular business hours, times when people are in meetings on break or at lunch, this is precisely when the *fraudster* calls again. As is the case with the receptionist who is normally on duty, a substitute’s job is to be helpful. When the *social engineer* calls he or she claims to be someone of importance. Using the knowledge acquired earlier, the *fraudster* is able to spin a creative story that seems plausible. The unsuspecting substitute responds to the *caller’s* request. The information that can be provided includes data that is within the

receptionist's access such as employee identification or health insurance policy numbers. Once information has been collected through *social engineering*, it can be used by the *fraudster* directly, sold or traded, or combined with other *breeder documents* to construct an *identity*. *Social engineering* can be used to steal information such as in corporate espionage [109].

Hal Berghel discussed *fungible credentials* which is a topic related to *social engineering* and the creation of false documents used to develop an *identity* [21]. In this scenario, once the *thief* obtains a piece of *identity* information, it is used as a seed to construct a highly useful and important *identity* document such as a fake passport. The false piece of documentation known as a *breeder document*, in turn, is used to generate additional *PII* such as a driver's license or social security number. *Identities* created in this way present law enforcement with significant challenges. The new *identity* and its offspring are present in a host of databases. Records exist for the *identity* in legitimate organizations and, because of the *identity thief's* attention to detail and the complexity of the *fraud*, can be verified. If someone becomes suspicious and attempts to check whether the person in question is who he or she claims to be, the *fraudster's identity* appears in numerous places which makes it appear to be authentic. Investigating the multiple false documents can require a significant amount of resources and creates a variety of related problems. Figure 7 shows Nevada licenses for Smith and Jones and is an example of this *fraud*.

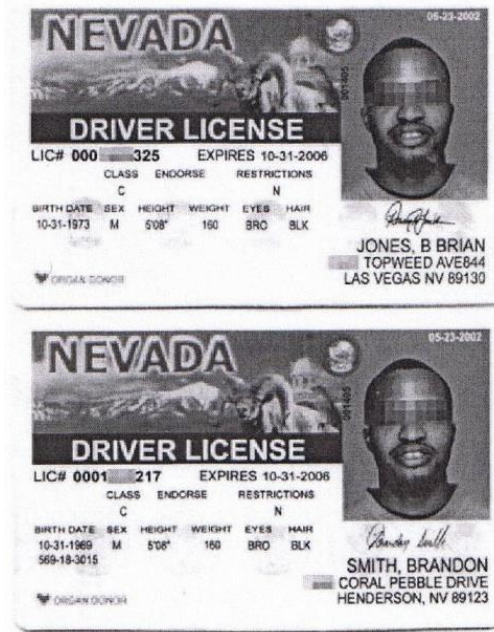


Figure 7: Smith and Jones Nevada Licenses

Section X Awareness

Public officials in other countries and the United States have been aware of the problem of *identity theft* for some time. In 1998 the U.S. Government passed the *Identity Theft and Assumption Deterrence Act of 1998* [175]. Its purpose was to expand, to clarify, and to codify legislation to deal with transgressions to the United States Code that relate specifically to *identity theft and identity assumption* [7]. “The United States Code is the codification by subject matter of the general and permanent laws of the United States.”[177]

The information in Table 1 reveals the predominance of the use of *breeder documents* in *identity theft* related crime. Material in columns one through three appears in the U.S. Sentencing Commission’s *Identity Theft: Final Report* of December 15, 1999. Statistics in the rightmost column reveal the relative percentage of *breeder documents* used for each offense with respect to the total number of the sample. The data shows that *breeder documents* contribute in a significant way to *identity theft* related crime.

Table 1: US Sentencing Commission *Identity Theft: Final Report, December 15, 1999*

Relationship of Breeder Documents to ID Means Offense Conduct

ID Means Offense Conduct	Total Number of Cases Involving This Conduct	Number of Cases Involving Breeder Documents	Percentage of Breeder Documents to Total Number of Cases
Credit Card Fraud	44	27	61.36
Check Fraud	36	13	36.11
Document/ID Means Counterfeiting	30	12	40.00
Immigration Document Fraud	29	4	13.79
Signature Fraud	25	12	48.00
Bank/Loan Fraud	22	11	50.00
Fraudulently Obtained Driver's License	13	12	92.31
Government Benefits	9	4	44.44
Trafficking in Fraudulent Documents	7	2	28.57
Tax Fraud	4	2	50.00
Firearms	3	2	66.67
Drugs	2	1	50.00

Appendix F from the U.S. Sentencing Commission's *Identity Theft: Final Report of December 15, 1999* contains a dozen illustrative summary examples of cases that highlight types of *identity dependent fraud*. Exploitations identified in the report included fictitious aliases, passport fraud, social security fraud, false statements, possession of another individual's *PII* such as birth certificate, driver's license or learner's permit certificate, misdirection and delay of mail delivery, opening mail, misuse of the telecommunications system, check, credit card and debit card fraud, securities fraud, stolen PIN numbers, hotel and automobile rental fraud, fictitious children, fraudulent loans, breeder documents, false employment and education verification, burglarizing homes and automobiles, conspiracy, and cellular phone fraud. A number of *scams* spanned extended periods of time, for example, as much as 18 years. Dumpster diving was a method used in some cases that did not require the unauthorized access of account information or a premises. Several *thieves*

were illegal aliens or had a criminal history that extended back in time several years time. Each example includes the number of offenses. In one case, 2300 fraudulent incidents of credit card, check and false identification were uncovered. Due to the number of compromises, no victims were contacted by law enforcement. In another case, the *fraudster* was in possession of more than 5,000 credit card numbers on hotel and car rental receipts. A small percentage of the *thieves* were imprisoned for their crimes. Sentences did not exceed 71 months. The majority of criminals received probation [176].

The U.S. Sentencing Commission posts updates regarding sentencing by region and other important material on its website. In 2009 the Commission produced *An Overview of Loss in USSG §2B1.1*. The document was designed to assist with sentencing guidelines and contains a number of definitions that include *loss*, *actual loss* and *intended loss*. In the document *loss* is defined to be the greater of *actual loss* or *intended loss* [174]. The term *loss* is used in the sentencing of *identity theft* related crimes.

Section XI Alarming Statistics

Research shows *identity theft* takes many forms, is increasing and that anyone can become a victim [14] [16]. *Identity thieves* are clever. They continue to reuse methods that they deem to be effective and to develop new strategies. The level of deception and the means that *identity thieves* use to obscure their involvement in the suite of interdependent crimes make combating *fraud* particularly challenging for law enforcement. As reports reveal, the penalties that *identity thieves* receive are, generally, light. On the other hand, the profit that they derive is substantial. The crime is lucrative and relatively simple to perpetrate. *Identity thieves* learn the vulnerabilities of their targets and are proficient in risk assessment. Statistics related to *identity theft* are staggering.

Latanya Sweeney reports:

“The US Federal Trade Commission’s (FTC’s) report on *identity theft* shows a rapid growth in victim complaints. Victims reported more than 86,000 incidents in 2001; this number grew to 162,000 cases in 2002, and rose to 246, 570 in 2004. More than a quarter (28 percent) of reported complaints involved credit-card fraud. Of the credit-card complaints, the report identified that approximately half (or 17 percent of all thefts) involved new accounts, making acquisition of new credit cards the major *identity theft* problem ...” [161].

Wenjie Wang, Yufei Yuan and Norm Archer state that:

“In the US, the number of *identity theft* cases reported to the US Federal Trade Commission (FTC; www.ftc.gov) grew from 161,836 in 2002 to 214, 905 in 2003, an annual increase of 33 percent. (www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf.) Some estimates in 2002 put the number of American *identity theft* victims close to 10 million, an 81 percent rise from 2001 and at a cost of nearly US \$53billion. Phonebusters, (www.phonebusters.com), a Canadian *identity theft-reporting* agency, reported that more than 14,599 Canadians became *identity theft* victims in 2003 (compared with 8, 209 in 2002) and at a cost of roughly \$21.8 million (compared with \$11.8 million in 2002; www.phonebusters.Com/English/statistics_E03.html). A major reason for the dramatic rise in *identity theft* cases is the explosive growth in Internet applications, making *identity* information more widely used and thus an easy target for criminals. Although *identity theft* has become one of the top legal concerns of the information age, the more dangerous aspect is how terrorists can use it to breach national security.” [183]

Identity theft continues to grow. Recent statistics suggest that the rate has not declined and that the crime has branched into many directions [31] [89] [102] [114] [145] [158].

Many crimes associated with *identity theft* such as *credit card*, *insurance*, or *mortgage fraud* to name a few are not reported, because the victim is possibly unaware that an event has occurred, is complacent, or is perhaps ashamed and feels in part responsible. Under reporting of crime that involves *identity theft* is a worldwide concern [9] [14] [15] [16] [106]. April 23, 2008 the BBC reported that the banking industry claimed 290,500,000 pounds in losses in 2007, but that their investigation revealed that *identity thieves* had been successful to the tune of 500,000,000 pounds, a figure that was nearly double what the banking industry had stated.

Another story that the BBC reported on the same day as the banking piece was about the underground market in stolen *identity* information sold or traded to be used for *identity theft* dependent *fraud*. The report highlighted a case of credit card information stolen near Christmas from *hackers* based in Pakistan. The piece revealed that compromised credit card numbers are typically used to buy high value easy to sell small electronic devices. *Fraudsters* purchase these items illegally and then quickly sell them for cash. In some cases funds are used to promote terrorism. The preponderance of cash transactions causes difficult conditions in subsequent follow-up and investigative work. Andrew Goodwill, *fraud* expert from The 3rd Man software company was quoted from *The Web Trade in Credit Card Details* that *identity theft* is “out of control”. It was, also, reported in the article that law enforcement in the U.K. is far behind many European countries and the United States in addressing *identity theft* related crime. The primary reason is due to the authorities not wanting to become involved, because of the overwhelming number of incidents. For this reason, the U.K. represents a desirable and fertile field to work in for *identity thieves*. The lack of investigations and prosecutions are good incentives for *fraudsters*.

For example, the BBC reported on April 21, 2008 that a terrorist ring with access to stolen credit card numbers, committed *fraud* using a number acquired from a 70 year old woman. Her information was taken from an ATM machine without her permission by the *identity thieves*. In this case, authorities said the *fraud* resembled an earlier *scam* that involved a group of terrorists who were associated with the Sri Lankan Tamil Tigers. Funds gained from *fraudulent* activity were used to promote terrorism [14]. Not all *identity theft* related crime is engineered to fund terrorism. *Financial* and *non-financial identity theft* may have no relation to terrorism. Other reasons include personal gain to steal funds or acquire a job in the victim's name to conceal a criminal past [31]. All cases are costly. On the side of business the need to absorb the cost of stolen goods that result from *fraud* is substantial. A 2011 report estimated that the *average* cost per *identity theft* ranged between \$2,800 and \$5,100 [130]. In 2014 an estimated 17.6 million people's identities were stolen in the United States [158]. This suggests annual losses on the order of 100 billion dollars. The crime continues to grow in popularity with devastating consequences [14] [15] [41] [79] [85] [105] [106] [108] [117] [176] [183]. It is worth examining the economic impact on the individual and on industry in more detail. In addition, understanding the relationships with *e-commerce* is important.

Section XII Individual, Business and Government

The passing of *The Identity Theft Assumption and Deterrence Act of 1998* had far-reaching and significant impact that benefited individuals who were victims of *identity theft*. In the case of an individual, until the enactment of *The Identity Theft Assumption and Deterrence Act of 1998*, a person had no protection under the law [175]. While weakened

and perhaps in desperate circumstances due to *identity theft* initiated credit problems, a non-corporate victim had little recourse. The United States Sentencing Commission report provided information from interviews that identified the range of losses for individual victims of *identity theft*. The sample showed that people were negatively affected to the tune of \$5,000-\$40,000 per person. *The Identity Theft Assumption and Deterrence Act of 1998* expanded the definition of the parties considered to be victims of *identity theft* to include individuals [175]. This represents a significant change.

Prior to the enactment of this law, when businesses suffered losses from *fraudulent* activities associated with *identity theft*, the companies affected were considered the sole victims of these crimes. The targeted industries do sustain significant financial ramifications. The direct loss of stolen products leads to a company being unable to process orders which, in turn, causes problems moving forward with the business plan. In combination, these issues contribute to a lack of trust and are costly. The United States General Accountability Office reported on *check fraud* losses in March 2002. The Government urged caution in considering the results of the study and cited the low response rate of approximately 11%. The reason offered by the Government for the limited response provided by the banks was the belief that financial institutions did not want to reveal the extent of their respective vulnerabilities to their customer and competitors. The Government's position was that *check fraud* is significantly under-reported. The available statistics are revealing.

“10 percent for community banks (assets under \$500 million)...
 16 percent for mid-size banks (assets of \$500 million to under \$5 billion)...
 27 percent for regional banks (assets of \$5 billion to under \$50 billion)...
 65 percent for superregional/money center banks (assets of \$50 billion
 or more).” [79]

Rebecca Mercuri reports:

“Estimates of U.S. losses have stabilized (since 2003) at approximately \$52.6B per year, with around 90% (or some \$47.6B) of this total being carried by businesses and financial institutions, and consumers shouldering the remaining 10% (around \$5B). Per incident, the average cost has been stated as \$10,200 for institutions and \$1,180 for individuals.” [108]

Government expenditures related to *identity theft* continue to increase. The actual losses due to attack by *fraudsters* and the growing dollar amount required for greater oversight for prevention, detection and prosecution are costly. The rise in the number of *identity theft* crimes calls for additional resources to support law enforcement. The United States General Accountability Office (GAO) examines branches of government to determine where improvements can be made to reduce loss. The GAO studied crime that involves *identity theft* for more than a decade. It reported research results and recommended actions that require investment to reduce *identity fraud*.

One area of recent work considers losses associated with *tax refund fraud*. In this *scam* using *identity theft*, the perpetrator misrepresents himself or herself by submitting a tax-return form early in the tax season for an actual person who is entitled to a refund. The advent of electronic filing and electronic deposit provide easy tools for the *fraudster* to misuse. Once deposited, the funds are removed by the *thief*. The person whose *PII* was stolen learns of the problem when he or she experiences difficulty receiving the refund, because according to the Internal Revenue Service (IRS) it has already been paid. Data reported by the GAO shows that the IRS estimated that \$25.6 billion in *identity theft* attempted *tax-refund fraud* occurred in 2014. Of the total amount, \$22.5 billion or 88% was

prevented or recovered. The remaining \$3.1 billion or 12% was paid in refunds. The GAO recommends action by Congress and the IRS to improve the tax service's *identity theft fraud* prevention capability in an attempt to save billions of dollars in losses [80] [167] [168] [169] [170] [171] [172] [173]. Other United States Government agencies such as the Federal Trade Commission, report not only on consumer complaints with respect to questionable business practices, but also on attempts by *identity thieves* to counterfeit government websites or run phone *scams* by impersonating IRS employees. The IRS does not call individuals on the telephone with charges of failure to comply with the tax code [56] [58] [59] [60].

Medicare.gov provides information about Medicare *fraud* via stolen *PII* [107]. The amount of *fraud* perpetrated with *identity theft* or *identity assumption* crime is staggering. In spite of the awareness of the serious consequences of these crimes and recommendations from various Federal agencies, in 2015 United States Government suffered a substantive data breach. Servers were hacked by the *fraudsters* located in China. The system compromise was extensive [55] [74] [113]. Medicare *fraud* is significant and believed to be underreported. It is difficult to combat. False claims have been publicized where physicians' identifiers have been used to fraudulently submit bills to Medicare. Determining bogus claims is problematic, because of the number of legitimate agencies that provide services to seniors [89] [102] [114] [145].

Section XIII E-commerce

Financial losses from *identity theft* are substantial and impact the world economy [5] [14] [15] [41] [74] [79] [85] [105] [106] [108] [117] [140] [148] [176] [183]. Annually, billions of dollars are lost as a result of crimes that involve *identity fraud*. Until recently,

little was done to curtail *identity theft* related *fraud*. To a large degree, brick and mortar as well as businesses engaged in e-commerce did not want to make public the extent of loss suffered from *identity fraud* crime. They preferred to conceal data to retain the trust of customers and to avoid leakage of information that a competitor might find useful. Unfortunately, losses were considered as part of operating expenses and passed on to the buyer in the way of higher prices for goods and services. Recently, the model has changed. Government regulations in the United States require business owners of compromised systems to notify, in writing, all potentially affected individuals. The new model, considers the possibility that *identity* information was compromised as a result of a data breach. Notification in writing to all affected parties is costly and acts as an incentive to the business community to improve security measures on their systems. Company leadership has attempted to do so. However, based on the number of reported cases that involve retailers alone such as Target, Neiman Marcus and others, more must be done [149] [162] [163]. Law enforcement is overwhelmed with the volume of *identity theft* related crimes.

In addition to the financial loss incurred from the initial *fraudulently* purchased items, the ongoing issue of the continued use of the stolen *identity* remains. Trust is affected which negatively effects commerce. Studies consider the related issues [42] [79] [117] [141]. With respect to *e-commerce*, a drop in consumer confidence related to fears of security and privacy issues affect corporate decision strategies [6] [154]. Concerns that consumers will change purchasing habits, because of a lack of trust are justified by the effect of the 2013 Target attack where 40 million credit card numbers were stolen. Subsequent Target sales dropped substantially [162] [163]. It is more challenging to learn the extent of compromise in

financial service institutions which report little information so as not to negatively affect customers' choices [4] [144].

Insiders in an organization represent a serious threat to security and confidence. Wells Fargo and its customers are one recent example. Over a period of years beginning in 2011 and culminating in 2016 with fines of \$185 million dollars and the termination of 5,300 bank workers, employees created unauthorized accounts and credit cards for actual clients then assessed fees to the bogus accounts and credit cards [45] [185].

On a perverse note, a thriving underground electronic network exists where stolen *identity* information is traded and sold with regularity [16] [65] [73]. Sources monitoring underground traffic confirm that *identity* information is a commodity that is bought, sold and traded routinely. *PII* such as social security numbers, addresses, telephone numbers, credit card numbers, and other information are moved through the underground trade network. *E-commerce* of this type represents a tremendous drain on the national and world economy.

Section XIV Laws that Impact *Identity Theft*

Several pieces of legislation in the United States impact directly or indirectly issues related to *identity theft*. The 1935 *Social Security Act* is one of the laws that is integrally linked to *identity fraud* [21]. In August of 1935, under President Franklin D. Roosevelt, the *Social Security Act* became law. Its original purpose of this Depression Era legislation was to afford financial relief to individuals of retirement age. A unique nine digit was to be assigned to each person entitled to receive benefits. The number was to be called the social security number (SSN). Over the years, the *Social Security Act* was amended to provide for a distribution of funds to survivors of the deceased as well as the disabled. The expansion of

resources to include these groups substantially increased the original program well-beyond its initial implementation.

President Roosevelt signed *Executive Order 9397* in 1943 which allowed social security numbers to be used as primary keys in other government branches' databases. This seemingly innocuous change that was designed to provide ready access to government benefits had a serious and unseen future consequence. As time moved forward, it created the means by which to link individuals to many pieces of *identity information*. For example, the SSN was used as the *identifier* to check books out from some libraries. The borrow history appeared on a slip of paper affixed to the inside cover of books on loan at libraries. Also, at one time the SSN was used as the contract number for health insurance coverage, so it appeared on the face of health insurance cards.

The Privacy Act of 1974 required changes in the use of social security numbers as primary keys in federal databases in 1975. The Act mandated that all government agencies, other than the Social Security Administration, provide a *Privacy Act Disclosure Notice* to a SSN holder that includes: (1) why they are entitled to the information; (2) the primary use of the information; (3) other possible uses of the information; (4) and the potential outcome of a compromise of the information. Also, it eased state and local disclosure restrictions which resulted when items (1) and (2) were combined with (3). Finally, the Act acknowledged the use of SSNs as a primary key for legitimate use by government agencies [21]. Latanya Sweeney relates issues In *Protecting Job Seekers from Identity Theft*:

“SSNs have evolved from being internal account numbers for the Social Security Administration into national identifying numbers for individuals living and working in the US today. They're essential for identifying, recognizing, and authenticating

people in health, financial, legal, and educational contexts. Amazingly, some people still believe that SSNs aren't publicly available. In 2003, the California-based Foundation for Taxpayer and Consumer Rights paid US\$26 each for SSNs and home addresses of some of President George W. Bush's top officials.⁵ Also, in 2003, the US General Accountability Office identified SSNs as ripe for terrorist exploitation, making such vulnerabilities a serious concern for homeland security and a grave threat to the country's economic prosperity." [161]

As indicated earlier, once recorded and stored electronically, data is no longer private [4] [21] [109] [183]. Following the enactment of the *Social Security Act of 1935*, *Executive Order 9397* in 1943, and the *Privacy Act of 1974* industry and business appreciated the value of the SSN as an identifier and supported its use. Over a period of time and combined with the repeated abuse of the SSN, it has become a common method for authentication. In turn, this has resulted in a substantial increase in risk of the loss of *PII*. The *fraudster* makes use of the ready availability of the SSN.

Improvements in computer networks and the ubiquitous nature of technology in today's society provide fertile ground for the *identity thieves* adept at stealing. The complement of crimes are easy to perpetrate, lucrative and associated penalties are minimal. They provide the *fraudster* with a steady and comfortable living.

Historically, industry transferred the expense from losses related to *identity theft* on to the consumer through higher costs of goods and services. However, this does not address the devastating consequences to crime victims. The Congress of the United States took action to criminalize *identity theft* in an attempt to assist and protect individuals from the barrage of problems associated with *identity theft*. The legislation created to address these challenges is *The Identity Theft and Assumption Deterrence Act of 1998*. It was enacted on October 30, 1998. A major piece of this legislation is that it expands the concept of whom and what

constitute victims of this form of crime. It acknowledges that a person can be a victim of *identity theft* as opposed to exclusively businesses. Before the *Identity Theft and Assumption Deterrence Act* was enacted, the United States government did not consider the loss of *PII* through theft as a criminal act against a specific person. Instead, the emphasis of existing legislation was to focus on the financial losses incurred by companies and other organizations. These entities were understood to be the only victims of *identity theft* since the monetary losses directly impacted them.

The view of the crime of *identity theft* and how it is perceived in the United States legal system has changed. The *Identity Theft and Assumption Deterrence Act* provides the necessary legal framework to protect individuals [175]. Significant fines and penalties are now in place. For example, if convicted, incarceration for up to 25 years is possible for certain crimes that involve *identity theft*. In addition to Federal legislation, all states have enacted *identity theft* laws. The laws address impersonation; forfeiture of goods obtained via *identity theft*; *identity theft* passport programs to protect victims from unfair treatment that can occur; buying, selling or trading stolen *identity* information; and protecting children through requiring annual credit reports and convicting parents of a felony if they steal their child's *identity* [1].

The United States passed the *Identity Theft and Assumption Deterrence Act* to address this growing crime. Other countries have moved in a similar direction. For example, the Government in Canada took action in January 2001 to mitigate the loss of *PII* through the enactment of the *Canadian Personal Information Protection and Electronic Documents Act* (PIPEDA) [183]. The legislation requires organizations to make a significant effort to protect and prevent the loss of clients' *identity* information. PIPEDA addresses the need for

security and for appropriate procedures to be in place to ensure sufficient levels of privacy in relation to the sensitivity of the information. Also, it requires that individuals with a genuine need to access sensitive information sign a confidentiality statement. In recent years the Federal Government in the United States passed additional legislation intended to protect the privacy of the individual and to require accountability from business. Examples include the *Health Insurance Portability and Accountability Act of 1996* (HIPAA) with the focus of privacy in the health care industry; the *Gramm-Leach-Bliley Act of 1999* (GLB) that requires privacy and security in the banking, securities and insurance industries; and the *Sarbanes-Oxley Act of 2002* (SOX) that addresses privacy accountability in industry [22]. These pieces of legislation carry severe penalties for those who abuse them. For example, in the case of SOX top level officers in the business must sign off on the creditability of financial reports so that the public is aware of the status of the company. Failure to provide truthful information can result in jail time for the administrators who are involved in providing false information.

Section XV Detection and Prevention

A variety of methods have been proposed over time designed to mitigate *identity theft*. Research addresses detection and prevention of crimes that rely on *identity fraud*. [4] [23] [27] [39] [40] [61] [62] [67] [85] [86] [87] [88] [103] [105] [115] [117] [121] [124] [130] [132] [136] [154] [183] [158] [187]. Strategies range considerably and focus on technical vulnerabilities, the introduction of the latest hardware or software improvements, and the deployment of new protocols to protect security and privacy of *PII*. Measures to promote the prevention and detection of *social engineering* via policy changes and education are also considered. Michael Benson discusses options in *Offenders or Opportunities: Approaches to Controlling Identity Theft* [19]. Work that focuses on detection and

prevention is extensive [23] [39] [41] [40] [44] [61] [62] [67] [85] [86] [87] [88] [103] [105] [115] [117] [121] [124] [130] [132] [136] [154] [183] [187]. In addition, many public service websites provide current and meaningful information to individuals. For example, a sample of government and non-profit organizations sites discuss a variety of topics such as detection and prevention and recovery after an incident has occurred [50] [57] [77] [78] [83] [120] [145] [164].

Detection and prevention methods can be subdivided into predominately technical and non-technical groups. In some cases, the two intersect. Areas include better access to information and education that concerns *identity theft*; the creation and deployment of protocols to address new and emerging technologies such as *biometric data*; the development of hardware and/or software tools; and the assessment of risk.

Considering detection solutions, education, software, and risk analysis can be grouped under this umbrella. Information provided by the Federal Trade Commission; Thomas Nagunwa; and Wenjie Wang, Yufei Yuan and Norm Archer examine these issues [40] [115] [183]. Other solutions that integrate software into the strategy are available in research papers from Dinei Florencio and Cormac Herley; and Ian Fette, Norman Sadeh and Anthony Tomasic, respectively [61] [62]. The latter offers a machine learning utility to detect *phishing*, while the former uses a statistical tool to determine the possibility of authentic password use at an unfamiliar website. Researchers Sarah Spiekerman, Jens Grossklags and Bettina Berendt as well as Sujata Garera, Niels Provos, Monica Chew and Aviel D. Rubin examine risk assessment [67] [154].

Prevention solutions include education, risk assessment, software and protocols. Researchers R. Clay Mathews and John E. Potter provide informative data to educate the

reader [103] [132]. Work that addresses risk assessment includes papers from R. Dhamija, J. D. Tygar, Marti Hearst; Sabine Delaitre; Markus Jakobsson and Jacob Ratkiewicz; and Julie S. Downs, Mandy B. Holbrook, and Lorrie Faith Cranor [39] [41] [44] [85]. The second of these papers considers *biometric data*. The other three studies examine and assess psychological issues that foster *identity theft*.

Solutions dependent on software are provided by Thomas Raffetseder, Engin Kirda, and Christopher Kruegel; Nicole Leeper Piquero, Mark A. Cohen, and Alex R. Piquero; Shingo Orihara, Yujio Tsuruoka, Kenji Takahashi; and Daveante Jones, respectively [87] [124] [130] [136]. The first paper identifies issues related a security tool ported to Microsoft originally designed to be compatible with Firefox. The second and third proposals incorporate the use of software for authentication. The last of the four papers examines how to protect *biometric data*. Protocols are considered by a number of researchers. A sample of several teams include Kun Lin, Lin Yuan and Gang Qu; Richard McMahon, Martin S. Bressler, and Linda Bressler; Paul Madsen, Yuzo Koga, and Kenji Takahashi; Min Wu, Robert C. Miller, and Greg Little; and Eleanor K. Jator and Kimily Hughley [23] [86] [88] [105] [121] [187].

Section XVI Other Directions

A variety of detection and prevention strategies have been proposed. Many integrate the use of technology into a solution. Software and hardware add-ons represent some possibilities. Some researchers have argued that the combination of these methods is viable as well. As *identity theft* evolves, it has expanded its tentacles into an ever greater number of crimes [79]. In March 2002 the General Accountability Office (GAO) reported troubling revelations in *Identity Theft: Prevalence and Cost Appear to be Growing*. The story has

worsened according to the GAO [167] [168] [169] [172] [170] [171] [173]. *Identity thieves* continue to exploit vulnerabilities from a wide array of directions so that they are able to steal resources. For this reason *identity theft* crimes can involve an intricate web of *fraud* such as *mail, financial, insurance, phone, online shopping* and others. Multiple oversight and jurisdictions often must unravel these crimes. For example, the United States Treasury Department, Federal Bureau of Investigation, and the United States Postal Service may work on a single case. The maze of deception is challenging to sort through or prevent.

Two other methods to combat *identity theft* focus on different approaches. They address prevention and what must be done after a person's *identity* has been stolen. *Identity theft* insurance is an evolving industry. Companies such as *LifeLock*, as advertised on television and radio, provide monitoring mechanisms before an event occurs to help prevent an individual from becoming a victim and resources after the fact to clean up the mess [4] [144]. A significant component of this and similar products is the continuous monitoring of a client's credit score [38]. The three reporting bureaus include *Equifax, Experian* and *TransUnion* [49] [51] [166]. A major purchase that involves credit must pass through one of these agencies. Any items bought using credit affects an individual's credit score. If no substantial purchases are made, credit scores should be similar on the three credit bureau sites. If an unusual action or actions that affect an individual's credit score occurs, companies such as *LifeLock* notify the client of the suspicious activity. It is possible that a change in credit score is the legitimate result of behavior initiated by a policy holder. However, if it is not, the client is informed immediately of the illicit activity in near real-time. Notification is provided via a variety of methods such as text-messaging and email. Because of the short time required for information to be forwarded to the client, it is possible

to address nefarious issues quickly. Frank Abagnale who is associated with one such company, *PrivacyGuard*, explains that regardless of the protection offered from *identity theft* protection products, a person's credit report can never be entirely restored to its pre-event status following a significant *PII* compromise [4] [135]. A mark remains on the victim's credit report linked to the *fraud* and remains in perpetuity.

Identity theft insurance is one proactive measure that is currently available to assist with mitigating *identity fraud*. However, it benefits only policy holders. Substantial improvement in education needs to take place to assist the general public. *Social engineering* provides valuable inroads for *identity thieves* [3] [4] [10] [29] [109] [110] [118] [144]. Psychological and social reasons have been examined that predispose people to be susceptible to methods of *identity thieves*. Strategies have been purposed to combat these attack vectors [6] [9] [41] [42] [44] [61] [62] [67] [84] [85] [106] [111] [115] [122] [130] [136] [154] [187]. Security experts argue that the need exists for established policies, meaningful training in the work environment and public education to slow the growth of *identity assumption* [3] [4] [109] [144]. More work must be done so that people understand the magnitude of the problem, see red flags and warnings that may be visible, and behave appropriately to help prevent *identity theft*. Changes by the individual, at the personal level, and in relation to how data is handled at the business level, can make a difference.

Section XVII Privacy versus Security

Computer privacy and security on networked systems presents challenges for *cyber specialists*. In spite of significant amount of resources that are made available to build robust computer networks, keeping confidential and personal information secure continues to be elusive. Reports of breaches in databases that contain *PII* such as financial, medical, military

or educational information have, unfortunately, become routine. Compromises such as these contribute to the growing problem of *identity theft*.

The number of people impacted by *identity fraud* and the related loss of resources involved is staggering [85] [108] [183]. Financial services continue to be the most sought after target by *identity thieves* according to APWG [9]. As the risk to financial institutions and other services continues to expand, improvements in security that include technical solutions and adjustments in human behavior are needed. Positive movement in the technical and non-technical directions, with a focus on prevention, is imperative. Of the two bodies of work, behavioral changes are likely the more difficult to accomplish. Technological schemes to provide electronic solutions are proposed on a regular basis. Many combinations of hardware, software, protocols and policy exist designed to provide security and, consequently, privacy [23] [27] [39] [61] [62] [105] [117] [121] [124] [130] [136] [165] [187]. Developing technologies such as *social network* sites provide new challenges [131]. Data breaches can affect security and privacy [72]. The significant problem remains, namely, how to convince system users of the importance and necessity to establish and practice strong security measures to prevent *identity theft*. System users include individuals whose *identities* are at risk of being stolen due to personal choices that may not be in their best interest or are related to their ignorance of the issues, and also members of the labor force such as employees of companies who have access to vast stores of *PII*.

Concerns that are raised in relation to privacy and security are real and important. As computer technology develops, does a reasonable balance between privacy and security exist? As *cyber crime* and *terrorism* expand, is Big Brother inevitable? Win Treese examines this issue and the potential loss of privacy [142]. Frank Abagnale and Kevin

Mitnick discuss the inherent weaknesses of security systems designed to keep data safe [4] [109]. The cyber security experts note the ease with which attackers can gain access to valuable *PII* via *social engineering*. Mitnick relates many cases in his book where this surreptitious method was employed. In a substantial number of *social engineering* instances an insider is the weak link in the security system chain. Research shows that 70% of compromised data is the result of actions by an insider. The insider can be a knowing participant in the *scam* who sought employment at an institution with the specific purpose in mind to gain access or an employee, sometimes near the bottom of a hierarchal command chain who is completely unaware of the *fraud*, or someone who is careless. Regardless, the *identity thief* exploits resources that are available to the insider. Dignitaries and celebrities are not exempt. For example, former presidential candidate Barack Obama's passport data was illegally viewed by Federal Government employees in the United States. Australian immigration authorities mistakenly sent passport information for President Barack Obama, Russian President Vladimir Putin, German Chancellor Angela Merkel and British Prime Minister David Cameron to Asian Cup football tournament organizers [12] [55] [156]. Data breaches such as these are typical and occur with a good deal of regularity.

Privacy is under attack from other directions, too. Researchers Tom Jagatic, Nathaniel Jobson, Markus Jakobsson and Fillippo Menczer discuss the availability of *PII* after it is posted on websites for social reasons [84]. Study results showed that participants resented the fact that their *PII* was gathered during the experiment by using methods under investigation. Some participants expressed concern and the belief that a violation of their privacy had occurred. Latanya Sweeney examined loss of *PII* [161].

Markus Jakobsson and Jacob Ratkiewicz reported that 47% or 44 out of 93 of test subjects did not use the internal email assigned to them designed to protect their privacy. Rather than doing what they had been instructed to do to communicate in the study, these people chose to use their real-world email accounts. In so doing they revealed their personal email addresses to unknown respondents during the phase of the research project where the simulated use of an online auction site called rOnl (pronounced “ROW-null”) was observed [85]. Alessandro Acquisti and Sarah Spiekermann, Jens Grossklags and Bettina Berendt consider the incongruity of study participants’ statements related to their desire for privacy and their actual behavior when afforded the opportunity to act in an *e-commerce* environment [6] [154]. The lack of security and privacy in relation to *PII* on *social networks* is vast and well documented. Tremendous amounts of material are available online from reputable and sources, but the problem continues to grow as more data is compromised [2] [52] [150] [151] [152].

Robert Kling’s collection contains work by a number of authors who have explored these issues [93]. Focus areas and points of view vary, but they all address the issue of privacy versus security. The articles include a cross section of ideas and consider topics such as surveillance and monitoring as they relate to legal issues and the possibility of abuse. Articles written by Andrew Clement *Considering Privacy in the Development of Multimedia Communications*; Dorothy Denning *Clipper Chip Will Reinforce Privacy*; Denison Hatch *Privacy: How Much Data Do Direct Marketers Really Need?*; Chris Hilbert *What to do When They Ask for Your Social Security Number*; Robert Kling *Information Technologies and the Shifting Balance Between Privacy and Social Control*; Robert Kling, Mark Ackerman and Jonathon Allen *Information Entrepreneurialism, Information Technologies,*

and the Continuing Vulnerability of Privacy; Richard Kusserow *The Government Needs Computer Matching to Root Out Waste and Fraud*; Kenneth Laudon *Markets and Privacy*; David Linowes *Your Personal Information Has Gone Public*; Robert Posch *Direct Marketing Is Not a Significant Privacy Threat*; Marc Rotenberg *Wiretapping Bill: Costly and Intrusive*; John Shattuck *Computer Matching Is a Serious Threat to Individual Rights* are thought provoking and relevant. The questions asked in these works need to be considered, particularly with the electronic storage of *PII*. The threat of compromise is serious. Long term consequences can be severe.

Cyber terrorism is another very real threat. It can impact privacy and security. Steffen Schmidt and Michael McCoy consider this case in *Who Is You?* [144]. Examples of *cyber terrorism* or *cyber warfare* are evident in attack are evident in cases where Russian attackers hacked and accessed information on Democratic National Committee computers prior to the 2016 Election in the United States [43] [54] [116] [137] [143]. *Cyber security specialists* from Symantec demonstrated the ease with which is possible to compromise voting systems in the United States. Some have argued that, because voting is handled at the local level, and that thousands of independent systems are distributed across the Country, that affecting the election process would be impossible. As *cyber security specialties* point out, notable vulnerabilities exist in these disparate systems. In reality, system wide compromise is unnecessary, but rather attacks targeted at specific swing voting areas. This strategy effectively reduces the number of computers required to impact an election [71] [123] [179]. Surveillance and its relationship to *privacy* and *security*, the law, and possible abuses are discussed by Richard Spinello in Chapter Five of *Cyberethics Morality and Law in Cyberspace* [155]. Sara Baase examines the issues in *A Gift of Fire* [10].

Articles by Fawzia Cassim, Patrick Kosciuk and Daveante Jones explore privacy in relation to security [32] [46] [87]. The discussion centers on the proposed implementation of a *National Biometric Identity Card* in the United States similar to those in use in European countries such as the United Kingdom, Germany, Poland, Italy, Greece and Spain. Another individual who opposes the use of *biometric security* measures with a *National Biometric Identity Card* is Fujawa. She argues against the adoption of *biometric data technologies* for security and discusses legislation and issues related to the loss of *privacy* that resulted following actions by the United States Government after September 11, 2001. Fujawa states that citizens of the United States have already given up substantial freedoms because of the changes in our laws. Kosciuk has mixed views. He opposes the adoption of a *National Biometric Identity Card* in the United States on the grounds that it would be a violation of *privacy*. However, he feels that *biometric data* for security purposes is inevitable and that the Federal Government should fund and have exclusive oversight in this arena. Woodcock's opinion is in direct contrast to Kosciuk's point of view. She believes that research and development must continue in this direction and that the adoption of a *National Biometric Identity Card* with personal information such as social security number, driver's license data, and credit card information is the way that the United States should go to maintain national security. Woodstock states, "no one can expect privacy when his own *identity* has been stolen and used against him." Her position addresses identification, regardless of the loss of privacy to enhance security in the United States. She feels strongly about the need to move forward with *biometric* technologies and a *National Biometric Identity Card*. Organizations such as the Electronic Frontier Foundation have long supported civil liberties argue against Federal identification cards and databases that contain *biometric data* [101]. Because

biometric solutions depend on access to data unique to an individual such as finger prints, retinal scans or facial impressions, they have great value for authentication purposes. However, if a database housing this information is compromised by *identity thieves*, the *attackers* “hit pay dirt”. *Biometric data* in hand, the *fraudsters* are able to access whatever resources are available to their victims. Because *biometric data* is involved, the challenge for the victim is to prove that he or she did not initiate the act in question.

In spite of innovative software and hardware solutions and new laws that are in place intended to protect and prevent *identity theft*, *PII* continues to be taken from computer systems. Hal Berghel recommends that executives be held accountable for data breaches and the loss of sensitive personal information similar to what is in place in the Sarbanes – Oxley Act (SOA) [22]. SOA was enacted following the collapse of companies Enron, WorldCom, Tyco, etc. at the end of the 20th century to protect consumers from questionable activities in the investment industry. SOA requires that executives sign-off on the company’s balance sheet to ensure that the books represent accurate information. If the recorded data proves to be untrue, executives can be held accountable, face time in jail, and be subject to substantial fines. Berghel suggests that incentives similar to SOA would provide motivation to CEOs to provide better protection for *PII* stored on company computer systems.

Identity theft is a major problem that society faces today. Its reach is long with complex tentacles that are difficult to combat. New strategies to fight the crime are necessary. After examining *identity theft* issues, it is now time to consider a new direction. The study of education through game-based learning is the focus of the chapters that follow. Chapter 2 discusses the design and development of the game-based educational software Fight Identity Theft (FIT).

CHAPTER 2

DESIGNING AND DEVELOPING AN EDUCATIONAL METHOD TO COMBAT
IDENTITY THEFT

Section I Another Direction

Earlier in this paper a variety of established methods such as hardware and software solutions, protocols and policy were discussed to address and combat *identity theft*. These directions have proven to be effective to varying degrees. However, as has been discussed, the problem of *identity theft* and its consequences are vast and growing. Rich resources are available online to inform the public of this devastating crime. However, many people remain uninformed and as a consequence represent “easy marks” for *identity thieves*. Additional strategies are needed to affect positive change in order to mitigate the problem.

Educational games have shown promise in numerous domains such as learner engagement and motivation as well as diverse content areas that range from mathematics, software engineering, and science to name a few [33] [99] [98] [104] [157] [186]. Because of the promise of educational games and the need for solutions to combat *identity theft*, the focus of this research is the design and development of resources to address the crime. This study will consider traditional versus contemporary learning methods, namely, text-based and game-based learning. The text-based component of the educational module in the research tool is similar to the way in which information is currently presented via the Internet. The game-based educational module contains the exact same information as presented in the text-based unit, but in a game format complete with audio, graphics, video, question and answer and scoring. Before describing the research project and relating it in context, background that outline game-based learning will be informative and useful.

Section II Games and Educational Games Why Games?

Games offer a variety of benefits to the player. Perhaps some of the first things that come to mind are that they are entertaining, engaging and fun. Games require skill and expertise that are, generally, acquired over time. A progression of tasks provides the player with knowledge that, in turn, allows the individual to develop and improve with repetition. Regardless of the content focus, problem solving is a key component in many games. Tasks through game play may become more challenging and consequently require the development of greater skill and expertise for continued success. The combination of the factors fosters motivation and the desire to learn. They are worth exploring and applying to *identity theft* education

Recently, video games surpassed the annual box office sale of tickets for Hollywood films. Statistics show that in 2010 more than 25 billion dollars were spent on video games in the United States. This figure is significantly higher than the 10.8 billion dollars paid for the combined movie theater tickets sales in the United States and Canada in 2011 [11]. Research shows that 97% of young people in the United States play one or more hours of video games on a daily basis. A significant number of studies have focused on the negative aspects of computer games [69]. The level of violence in some computer games has raised questions and concerns. The depth and complexity of games has evolved over the last 15 years. This change is possible because of advances in technology and the associated reduction in cost that subsequently allow for ever greater and more sophisticated design elements to be incorporated. Entire worlds can be constructed by players in essentially real-time. Video or digital games are dynamic. They share a common theme, namely, that they are interactive.

Challenges in combination with rewards can provide the player with a stimulating and engaging environment to explore [11] [69].

The field of digital educational game development is evolving. Because of the motivation value, it might be expected that electronic educational games are widespread. This is not the case, in part, for social and economic and reasons. There exists a common misconception by some that learning cannot be fun. Also, development costs to bring products to market affect decisions. Content appropriate for different levels of students must be marketable in order to recoup expenses and to make a profit. No considerations for the foundations of education are necessary for entertainment games. Because of the need for greater *identity theft* awareness, it is worth considering and exploring alternatives to address education. Before discussing the design and development of this project, it is important to understand the educational foundations of game-based learning.

Section III Learning Foundations

Psychology affords numerous learning theories that have developed over time. Cognitive sciences have evolved over the past 30 years as a result of researchers working in conjunction with educators in classrooms to assess the efficacy of their theories. One significant area of development involves the merging together of different areas of science. New areas of research include (1) the study of competence and how knowledge is organized, both of which are fundamental in problem solving; (2) learning and how it is transferred to new settings; (3) the role that cultural background and mores play in learning; (4) how learning affects the brain's structure; (5) assessing learning environments and the impact that the setting makes; (6) and new technologies.

Toward the end of the 19th century, the study of learning moved from the domains of theology and philosophy to the realm of science where analytic tools and systematic methods were developed to study the mind. By the early 20th century *behaviorism*, had emerged with the creed that in accordance with scientific method, that the study of psychology must be limited to only observable behaviors in association with stimulus in a controlled environment. This represents a significant change from the past and is at the heart of today's learning theories in which empirical data are required [76].

Game-based learning, dependent on computer technologies, is an emerging area. Learning theory, in general, is a relatively new science. Its foundations are found in the cognitive sciences that include *behaviorism*, *cognitivism*, *humanism*, and *constructivism*. Research in these disciplines that affect game-based learning is ongoing and contemporary. It is important to integrate learning theory principles into educational games. The need for effective games to address *identity theft* education cannot be understated.

Behaviorism includes three tenets: *direct instruction* from Engelmann [47]; *programmed instruction* from Skinner [63]; and *social learning theory* from Bandura [182]. The first of these principles, *direct instruction*, advocates learning by listening to lectures. The second principle, *programmed instruction*, proposes learning by self-teaching methods. The third principle, *social; learning theory*, suggests learning from others through imitation, modeling and observation.

Cognitivism asserts four principles that include: *attribution theory* from Weiner [184], *elaboration theory* from Reigeluth [139], *stage theory of cognitive development* from Piaget [129], and *theory of conditional learning* from Gagne [66]. The first of these principles, *attribution theory*, relates that learners attempt to make sense of their world by

fixing cause to an event, either external (outside force) or internal (personal responsibility). The second of these principles, *elaboration theory*, stresses the need that material to be learned should be organized from basic fundamental components through those that are complex. The third principle, *stage theory of cognitive development*, describes four universal developmental stages in children that include *sensorimotor*, *preoperational*, *concrete-operational*, and *formal operational*. The fourth principle, *theory of conditional learning*, purports the existence of five types of learning that include *attitudes*, *cognitive strategies*, *intellectual skills*, *motor skills*, and *verbal information* and that each one requires different external and internal prerequisites for learning to occur.

Humanism from Combs and Huitt evolved post 1960s with the central position that learning should be individualized and student centered [34]. *Humanism* has one principle, *experiential learning* examined by Kolb, that states understanding is determined entirely by the individual via first-hand experience [94]. In 1985 Kolb proposed four different learning styles that include: *diverger* (preponderance of concrete experience in combination with reflective observation), *assimilator* (abstract conceptualization coupled with reflective observation), *converger* (abstract conceptualization in combination with active experimentation) and *accommodator* (concrete experience coupled with active experimentation).

Constructivism, *the fourth theory*, has eight principles that include: *social development theory* from Vygotsky [181]; *case-based learning* from Powell [133]; *cognitive apprenticeship* from Brown *et al* [30]; *discovery learning* from *Learning Theories Knowledge Base 2008* [159]; *problem-based learning* from Walker and Leary [48]; *situated learning theory* from Lave and Wenger [97]; *activity theory* from Leont'ev [100] and

Vygotsky [180]; and *actor-network theory* from Latour [96]. The predicate of *constructivism* is that individuals build or construct their personal understanding from objective reality by applying new information as it becomes known from Bednar *et al* [17]; from Resnick [90]; and from Brown *et al* [30]. In the first principle, *social development theory*, Vygotsky argued that language, written and spoken, is instrumental in the development of culture and, in turn, to its use in the reconciliation of societal concerns. Also, Vygotsky proposed a *zone of proximal development (ZPD)* which refers to the degree of assistance required by a student from his or her instructor or peers in relation to his or her ability to solve the problem alone. Vygotsky believes learning occurs in the ZPD. The mechanism employed to assist students in learning is known as *scaffolding learning*. *Case-based learning*, the second principle, branched off *constructivism*, and is a proponent of apprenticeship whereby the individual is actively engaged and learns by doing. The third principle, *cognitive apprenticeship*, calls for students to be exposed to real-world activities and practices via social interaction in order to solve problems through task-based learning. *Discovery learning* is the fourth principle and advocates for investigative instruction in which learning takes place in a *constructivist environment*. The work of Piaget, Bruner and Papert support this principle from Mayer [178]. The fifth principle, *problem-based learning (PBL)*, emerged as a result of education in medical schools in the 1960s. The focus is to provide students with authentic real-world problems to solve that may possibly require group work, cross-disciplinary action, and resemble true circumstances found in the profession. The sixth principle, *situated learning theory*, according to Fox [64] proposes that learning occurs within structured educational systems as a result of the behaviors of educators. It is understood that learning is not deliberate and that it is woven into the fabric of activities,

circumstances and culture. *Activity theory*, the seventh principle, is founded on anthropological and psychological theories. Kuutti [95] described its application with respect to computer technology in 1994. *Activity theory* is a philosophical structure to understand the growth of human culture and personality according to Bødker [26]. The eighth and final principle, *actor-network theory*, was developed by the *Learning Theories Knowledge Base 2008* [159] to assess technological achievement and scientific understanding. Its focus is on the relationship within a network and where vulnerabilities exist in human and non-human systems. The four learning theories discussed here and their respective associated principles are available in Figure 8 [188].

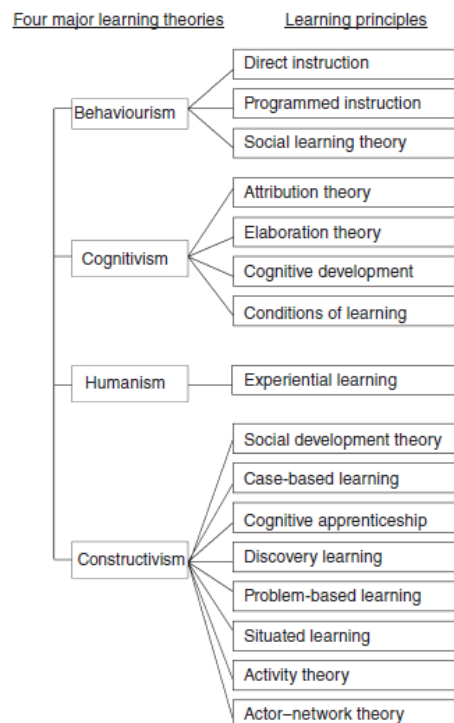


Figure 8: Four Learning Theories and Principles

The incorporation of learning theory principles into digital game-based learning is of fundamental importance. As integral elements of the game design process, they can assist in the development of a robust learning environment. This is needed to produce effective *identity theft* education tools. For example, *programmed learning* and *modeling* are tenets of *behaviorism* that can be incorporated into game-based learning. Similarly, from *cognitivism* *elaboration theory* and *conditional learning* can be applied. *Experiential learning* from *humanism* addresses the need for individualized learning. Principles of *constructivism* such as *discovery learning* and *problem-based learning* can contribute to game design. These principles represent cornerstone of learning theory and need to be integrated into game design.

Not all game-based learning tools are designed and constructed with learning theory as the central and guiding component. Researchers examined 658 studies of game-based learning and found that just 91 of these or 13.83% were predicated on learning theories. This represents a significant void and is of concern to members of the research community that stress the need for a strong basis linked to foundational theory [188].

In Chapter 3 *Simulation and Games in the Classroom of Learning Science Through Computer Games and Simulations* researchers present opportunities that exist via the use of educational computer games such as individualized learning and free instructor time to support learning. Also, that fact that educators can supply developers with much needed feedback related to students' misconceptions is suggested.

In Chapter 7 *Research Agenda for Simulations and Games of Learning Science Through Computer Games and Simulations* researchers discuss the positive impact of computer games and simulations. They address the importance of motivation and

engagement in achievement in the learning process. Also, they discuss the need for more research on *transference* and suggest three specific areas of investigation that include: how context affects learning; how learning is transferred from simulations or games to other environments; and the resilience of learning over time through longitudinal studies. In addition, consideration should be given to research that examines the potential for game-based learning in diverse communities [75].

Instructional technology has enjoyed an uptick in development and study over the past three decades. Software developers and scientists are working to integrate and expand the hands-on capabilities of technology into the learning environment. At the same time, they are committed to staying true to principles of learning theory. The concept of play in relation to instructional technology has received little consideration. This may, in part, be the result of inaccurate beliefs such as that play is unrespectable, easy and of no consequence in the learning process. None of which could be farther from the truth. This is in direct contrast with the fields of anthropology, education and psychology where play has been assessed in relation to its importance to learning and socialization.

One definition of play is that it is voluntary, self-motivating, requires effort, and has an imaginary quality from Blanchard and Cheska [25]; Csikszentmihalyi [36]; Pellegrini [125]; Pellegrini, and Smith [126]; and Yawkey and Pellegrini [189]. Contemporary play theories are grouped in four categories that include play as progress, power, fantasy and self. Play as progress relates to learning something of benefit, for example, experiencing growth in an area such as psychology. Play as power is associated with competition where there exist winners and losers. Play as fantasy affords the participant the opportunity to “think out of the box”, to try new things. Play as self stresses the importance of involvement in an event.

Three philosophies of education have enjoyed support over time and include *essentialism*, *progressivism* and *existentialism*. *Essentialism* mandates a top-down approach where an “expert” is deemed the sole provider of information that is deemed important that everyone needs to know. Play has no place in this philosophy, since the learner is expected to retain what is espoused by the “expert”. *Progressivism’s* tenets are based on the work of John Dewey where learning must be of value to the individual and be relevant. In this case, the “expert” and student work together to formulate a learning plan that is meaningful for the learner. Play is consistent with this model. *Existentialism* purports that no agency can make decisions that concern what any group should learn. Few rules exist in this model, so it is essentially represents *educational chaos*.

Flow Theory, an individual-centered learning theory proposed and studied by Csikszentmihalyi, contains eight key elements. They include that learner challenges must be maximized; that the learner must be completely engaged in an event; that tasks within the activity must have certain goals; that feedback must be direct and clear in relation to goals; that the learner must be, if only briefly, completely absorbed; that the learner is entirely in command of the event; that the learner’s self awareness vanishes; and that the passing of time proceeds unnoticed during the activity. These points identified in *Flow Theory* are in agreement with the precepts of gaming [138].

Mark Prensky is an advocate of game-based learning. He discusses his view of digital games in *Chapter 5 Fun, Play, and Games: What Makes Games Engaging* from *Digital Game-Based Learning*. In his opinion, computer games include 12 items that individually contribute to the experience. He examines how the 12 elements relate to computer games and their importance in learning. Prensky states that fun is a relative term

and that it may involve discomfort. He quotes Benjamin Franklin and Sivasailam Thiagarajan, two individuals' whose positions support his own, essentially, "no pain, no gain" The 12 elements include:

- “ 1. Games are a form of fun. That gives us enjoyment and pleasure.
2. Games are a form of play. That gives us intense and passionate involvement.
3. Games have rules. That gives us structure.
4. Games have goals. That gives us motivation.
5. Games are interactive. That gives us doing.
6. Games are adaptive. That gives us *flow*.
7. Games have outcomes and feedback. That gives us learning.
8. Games have win states. That gives us ego gratification.
9. Games have conflict/competition/challenge/opposition. That gives us adrenaline.
10. Games have problem solving. That sparks our creativity.
11. Games have interaction. That gives us social groups.
12. Games have representation and story. That gives us emotion.” [134]

Prensky, also, discusses the evolution of computer games; the change in level of interest in the sexes to play games over time; and work that industry promotes in order to appeal to different demographic groups.

The development of digital educational games that focus on *identity theft* and related *fraud* benefits from work such as Prensky's in game-based learning. His work suggests that opportunities exist to expand the educational environment so that it becomes immersive and engaging. The twelve elements are critically important. They need to be incorporated into digital educational games to provide the necessary solid foundation to address *identity theft* instruction.

The concept of *flow* is associated with researcher *Mihaly Csikszentmihalyi*. A main premise is the importance of *intrinsic motivation*, to seek to attain knowledge for its own

sake. Another key tenet is the requirement of *enjoyment* to facilitate learning. He discusses the relationship between *intrinsic motivation* and *flow* with respect to the challenges of education. According to *Csikszentmihalyi* without *enjoyment*, *flow* is not possible and consequently learning is limited. He maintains that subject matter and classroom structure, in suitable measure, are necessary for *flow* and *intrinsic motivation* to occur [35]. *Mihaly Csikszentmihalyi* proposed that a relationship exists between *skill level* and *challenge level* with respect to *flow*. The information is represented graphically in Figure 9. As one looks from left to right and from top to bottom, *skill level* and *challenge level* increase toward *flow*, the state of *enjoyment* where time stands still and the individual is totally engaged. This is the place where *Csikszentmihalyi* believes learning occurs most effectively [41].

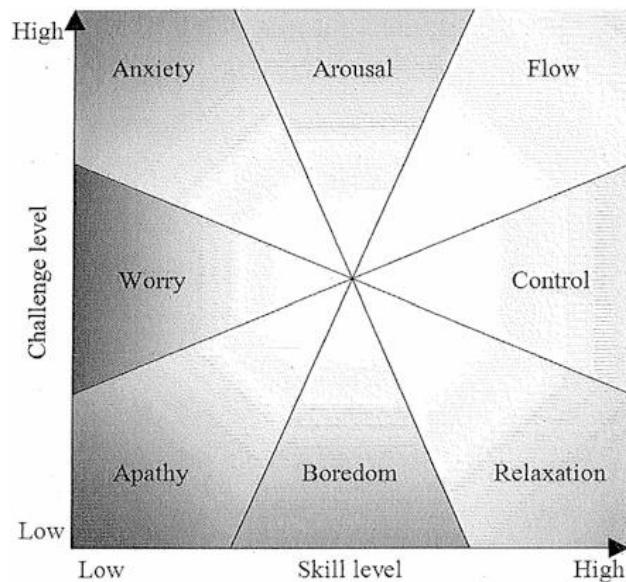


Figure 9: Relationship between Skills and Challenges

Educational computer games, with their vast variety, complexity and interactive capabilities offer opportunities to move into the realm of *flow*. The premise is that enjoyment associated with learning has positive and long-lasting effects.

Mihaly Csikszentmihalyi's flow is seminal in contemporary learning theory. The awareness and integration of appropriate levels of challenge and skill can help to produce effective digital educational games. The ultimate goal is to better educate individuals about *identity theft*.

Researchers in the field Chung-Ho Su and Ching-Hsue Cheng; Jeng-Chung Woo; Yu-Hao Lee, Norah Dunbar, Keri Kornelson, Scott Wilson, Ryan Ralston, and Milos Savic, Sepideh Stewart, Emily Lennox, William Thompson, Javier Elizondo; Lai-Chung Lee and Kuang-Chung Hao; Anuradha Mathrani, Shelly Christian and Agate Ponder-Sutton; Meng-Tzu Cheng, Hsiao-Ching She, and Leonard A. Annetta have explored digital game-based learning in a wide array of content areas that include software engineering; motivation, cognitive success and performance; mathematics; humor and animation; computer programming; and science [33] [98] [99] [104] [157] [186]. Their reports represent a sample of ongoing contemporary work in digital game-based learning. Student engagement and learning of substantive material is the focus. The results from their studies show positive results in this evolving field.

Section IV Assessment

In *Chapter 4 Games, Learning, and Assessment of Assessment in Game-Based Learning: Foundations*, Valerie Shute and Fengfeng Ke review six key properties and seven core elements that they believe are necessary for good games. They discuss games as transformative learning tools. Also, the researchers consider assessment of learning with respect to games. The work that they present supports the premise that games can be used to facilitate learning and that the results can be measured. Four studies of game-based learning

that require different kinds of participation are considered. The games/game categories include *Civilization*; *Gamestar Mechanic* and *System Thinking*; *Epistemic Games* and *Taiga Park and Science Content Learning* [147]. In the case of *Civilization*, learners gain knowledge of important facts and a significant understanding of the relationships between economics, geography and history in context. The focus in *Gamestar Mechanic* is on students' acquisition of thinking skills, in other words to examine the world in the "big-picture" rather than as a collection of distinct objects. *Epistemic Games* provide the learner with a virtual experience of real-world activities similar to those of professionals employed in the respective fields. *Taiga Park* is an immersive digital game set in a national park where diverse groups exist with different interests. The goal is to investigate and to solve issues that result from conflicting interests. Shute and Ke examine assessment reports for outcomes based on an *evidence-centered design* (ECD) and *stealth* methods. ECD is a design structure that offers developers a framework for game development and includes three models: competency, evidence and task. *Stealth assessments* are ECD-based assessment in which the assessment is unseen and is included as an integral part of the game. In this case, assessment does not hinder game flow [147].

In *Assessment in and of Serious Games: An Overview* Francesco Bellotti, Bill Kapralos, Kiju Lee, Pablo Moreno-Ger, and Ricardo Berta discuss the state of games as learning tools in relation to assessment. Issues are examined that reflect the difficulty of valid assessment due, in part, to complex and sometimes intangible outcomes. The researchers propose that rigorous guidelines, consistent with accepted principles, be mandated in order to establish the validity of assessment in game-based learning. They stress the importance of reporting learning progress as well as outcomes which includes player feedback. The need

for individualization to facilitate individual learning styles is discussed, also. Bellotti, et al. considers other researchers' work in this area. They offer methods to determine the effectiveness of game-based learning on the acquisition of competence and skills. Also, they offer suggestions for additional work in the field that includes identifying players' actions and greater integration of assessment into games. Three major types of assessment are discussed and include: competency assessment, in-progress assessment, and teacher assessment. These three tools reflect assessments that are summative, formative and whether a player completes the game, respectively. A variety of applications are discussed. The most common of which employs post-assessment such as surveys, tests, questionnaires, or instructor evaluations. Additional assessment methods are discussed as well [18].

Yoon Jeon Kim and Valerie J. Shute; and Sarit Barzilai and Ina Blau discuss elements of assessment in *The Interplay of Game Elements with Psychometric Qualities, Learning, and Enjoyment in Game-based Assessment* and *Scaffolding Game-based Learning: Impact on Learning Achievements, Perceived Learning, and Game Experiences*, respectively [13] [91]. Kim and Shute examined components of game-based learning that include *validity, reliability, fairness, and enjoyment* with respect to changes in *linearity*. The term *linearity* is defined as the degree of control or freedom afforded to the game player. In this study two versions of the same game were administered, one that was linear and the other that was nonlinear. In the case of the "linear" version players were restricted in movement through the game. Players of the "nonlinear" version had significantly greater freedom to make choices and pursue options in the game. Results showed that players of the "nonlinear" game showed marked improvement between pre-test and post-test assessments with respect to the qualitative understanding of content. In the second study, Barzilai and Blau examined

associations learned from material in the game environment to content learned outside the game. The researchers studied the effectiveness of the use of an external *scaffold* in conjunction with a game. They looked at three combinations that include “*study and play*”, “*play and study*” and “*play only*”. In the first case, the scaffold was examined prior to play. In the second case, the *scaffold* was reviewed after play. In the third case, the *scaffold* was not used. Results showed that learners with access to the *scaffold* before play performed better on the problem-solving activity following the game. Also, the scaffold did not negatively affect *flow* and enjoyment of the game.

A substantial body of work exists that focuses on the efficacy of game-based learning. Recently, studies have examined the importance of game design in relation to effectiveness. Matthew Gaydos in *Seriously Considering Design in Educational Games* suggests the need to codify educational game design in order to improve educational game research and development. He offers a definition of design as “*reflection-in-action, in which designers draw connections between the immediate design problem and their own experiences, relying on repertoires of design they have built up through professional practice or experience.*” He explains that as a practice, it can be improved. Also, Gaydos advocates for the sharing of game design in order to facilitate much needed consideration and critique [68]. In *Gameplay Engagement and Learning Game-Based Learning: A Systematic Review*, Azita Iliya, Abdul Jabbar, and Patrick Felicia consider game-based design with respect to engagement and learning. They examine the shortage of research as it relates to the effect of game design on learning results. Iliya et al. examine how game design affects engagement. They offer a framework of suggestions to be used in the design of educational games. They discuss the

cognitive and emotional impact of game-based learning as well as current trends in gaming [81].

Recent research suggests the value and importance of digital game-based learning. Theory and tools have evolved beyond the scope of computer-based training utilities. Current technology affords the mechanism necessary to construct robust learning environments. Creative alternatives to address *identity theft* education need to be considered.

Section V Research Design

For reasons outlined earlier regarding the exponential growth of *identity theft* and related problems that it promotes, the focus of this research is to provide educational information to the public. The importance of informing the people of the related issues cannot be overstated. Vast arrays of statistics, warnings, case studies and other materials are available online, as periodicals and in other forms to provide information to individuals about *identity theft*. In spite of the availability of data, the problem continues to grow. The ramifications of *identity theft* are dire. It is necessary to reach as many people as possible to combat the crime. Game-based learning can be used to help connect the public with information that they need to know. For this reason, a new alternative delivery method to provide information is suggested, namely one predicated on game-based learning.

Engagement and enjoyment are fundamental to achieving desired outcomes in this environment. In other words, *flow*, is necessary. Evidence from recent studies examined game-based learning in a variety of content areas unrelated to *identity theft* education supports this position. The need for better education with respect to *identity theft* is the reason for the development of *Fight Identify Theft* (FIT). Empirical evidence is necessary to

determine the usefulness of game-based learning in this area and is the foundation of this study.

Because college students are targeted by *identity thieves* for reasons outlined earlier, this population was chosen for the focus of this study. Pieces of demographic data will be collected that include age level, education level, major, self-assessment of the individual's technology understanding and sex (Appendix C). In addition, the total time a participant accesses FIT will be recorded. Prior to and following exposure to one of the two *educational modules*, study participants will be asked to respond to Survey 1 (pre-educational survey) and Survey 2 (post-educational survey), respectively. Surveys include nine questions about *identity theft* that can be answered in one of three ways that include *true*, *false* and "*don't know*". Correct answers to these questions are either *true* or *false*. The nine questions examine three categories that include the participant's prior misconceptions about *identity theft*, his or her lack of understanding of the consequences of *identity theft*, and jargon (Appendix D). Scores for each question on Survey 1 and Survey 2 are earned based on the participant's movement with respect to the correct answer. For example, if the actual answer to a question is true and a participant answers "*don't know*" on Survey 1 and *true* on Survey 2, he or she receives a score of 1 on that question. If on the other hand, on the same question a participant answers "*don't know*" on Survey 1 and *false* on Survey 2, he or she receives a score of -1 for that question. The complete scoring system is available (Appendix I). In addition, participant feedback will be recorded that includes benefit level, enjoyment level, and open text responses with respect to the participant's experience in FIT (Appendix F).

To assess the efficacy of a game-based learning with respect to *identity theft* education, two distinct computer-based educational modules are considered with study

participants exposed to one of these resources (Appendix G, Figures 10.a – 10.aa). The application will randomly select and assign each participant to exactly one of the two educational modules. One module is text-based, much like information that can be obtained in informational documents or online. The other educational module is game-based that contains questions and answers (Q & A), a point scoring system, graphics, audio, video, and puzzles to solve. Participants' results from the two delivery methods are compared. The same nine areas of content are presented in the two different systems that include *Communication, Education, Entertainment, Finance, Health, Home, Mobile Devices, Shopping, and Work* (Appendix E).

In the text-based delivery method, resources are presented in a typical computer format where the user makes a selection from one of the nine areas followed by information being displayed on the screen. Each panel contains six paragraphs of related text. The participant accesses informational material through reading. The learner can remain on a screen as long as he or she desires and can return to any screen to reread or review the content. The participant exits the educational module when he or she is ready to terminate the session.

The game-based-module provides the same nine areas as what is available in the text-based module, but it is presented differently. Rather than nine panels that contain six paragraphs, in the game-based module each of the six content areas is separated and presented as a single panel along with a Q & A format where points are awarded for correct responses. The delivery method within each of the six topic areas differs as well. Three panels contain a paragraph of text followed by a Q & A. One panel provides information via an audio recording followed by a Q & A. The recording on this screen can be replayed as

often as the participant elects to do so. Another panel includes a word-search puzzle of related terms along with a Q & A. Finally, one panel contains a video followed by a Q & A. The video can be replayed as many times as the participant wants to view the clip. The participant determines when he or she is ready to exit the application. Once the participant opts to end the session, data recorded during the application run is written to a file for later analysis.

Appendix G Figure 10.a through Figure 10.aa show screen shots of the text-based and game-based educational modules of FIT. Content provided in these two different delivery systems addresses issues that involve *identity theft* included in the pre- and post-survey questions. The initial screens of the text- and game-based areas are displayed in Figure 10.b and Figure 10.a, respectively. The next nine screen shots, Figure 10.c through Figure 10.k, show the text-based informational panels. Each one contains six paragraphs of material about *identity theft* (Appendix E). With the exception of the last screen shot, Figure 10.aa that displays the “Thank You” message to participants, the remaining images represent a sample of what the participant experiences during the game-based educational module. Additional detail outlining content displayed on the game-based panels follows.

Appendix G Figure 10.l through Figure 10.s is a group of screen shots for the *Education* option. Figure 10.l displays the video panel for this area. It has a point count of five. Figures 10.m, 10.n and 10.o are a set of images that show intermediate stages on the *word search puzzle* panel. The associated question has a point count of six. Figures 10.p, 10.q and 10.r are screen shots of single distinct questions with a value of one point. Figure 10.s displays the audio panel that has a point count of seven. Figures 10.t through 10.w show intermediate stages of the Main Game Board screen. The Main Game Board contains all

relative game information for the participant. Included are score in the game, percent of correct responses, points needed to reach the next level and the number of questions remaining in each of the nine content areas. Information is updated each time a participant completes a question. Figures 10.x and 10.y are sample feedback provided to the participant for correct and incorrect responses to questions in the game, respectively. Figure 10.z shows the last screen shot of the game, if the participant attempts all questions.

Appendix G panels share a common background and text colors. These were selected, because they are easy to view. Obtrusive colors or those that may affect participants' decisions were avoided. The nine colors used for text that is displayed on the menu for the text-based educational module, correspond to the background colors on the Main Game Board for each of the clickable options. The nine graphics used, one per text-based panel, appear on the Main Game Board Screen as selectable icons. On the game side, for all nine areas, each of the six panels has an appropriate graphic that emphasizes the issue that is addressed. The selection process for these images required a significant amount of time.

Appendix G game-based educational panels are designed with embedded learning theory fundamentals. They are interactive, engaging and promote *flow* in various ways and on different levels. *Flow* is an integral component of FIT. Mihaly Csikszentmihalyi's work is well-documented. The importance of maintaining a suitable balance of challenge and skill in the learning environment is imperative. A variety of delivery methods are employed to stimulate interest and to encourage participants to continue. Question weights are assigned with respect to the activity on the associated panel. One point questions are Q & A style. Videos, word search puzzles, and audio panels are weighted more heavily, because clues

require greater challenges and a higher degree of engagement. For example, listening to and understanding a clue is more difficult than reading and matching text to determine a correct answer, so the points assigned for a question with audio information are higher.

Appendix G questions in the game-based educational module have three possible answers, *true*, *false*, and “*don’t know*”. In the case of scoring within the game, points are awarded for correct responses that include *true* or *false*. Answers of “*don’t know*” are considered incorrect. If a participant’s selection matches the correct answer, points are earned. If a participant’s choice does not match the correct response, no points are earned. In either case, the participant’s score is updated and displayed on the Main Game Board. The subsequent related score calculations reflect the current state of the game.

Another design feature that promotes engagement is integrated into the Appendix G game-based module Main Game Board. Several intermediate screen shots are included that show changes to the Main Game Board through the different levels of play. As the game progresses, the amount of points required to move to the next level increases and, thus, provides a greater challenge. This, along with the reminder of the number of points needed to reach the next level and the updated score, are incentives to do well. The number of questions is fixed. It is important to answer correctly through the entire game in order to acquire the points that are needed to advance into the different levels.

Finally, incorporated into the design of FIT, again to promote engagement and *flow*, are numerous, interesting and appropriate sounds. The sounds provide another level of stimulation beyond purely visual content. As with the audio and video clips, they are intended to address different learning styles and to help focus the participants’ attention on the game. The amount of time required to assess and to select these sounds was substantial.

On the text-based side of the application, mouse-clicks are the only sound used until the final “Thank You” message is displayed. The same “Thank You” message is presented for both educational modules. On the game-based side, many diverse and suitable sounds are included. Design decisions were made to enhance the experience. They are intended to be entertaining, relevant and to be *fun*. Each of the nine areas to explore has a specific and unique sound associated with it. For example, on entering *Education* John Glenn’s message from his Moon walk is played. If the *Shopping* area is selected, a cash register sound is heard. If the *Work* icon is chosen, a fax-machine sounds. On the *word search puzzle* panels, “Hoorahs” are played when a puzzle is completed. On the participant feedback panels for correct and incorrect responses, applause and baby cries are played in conjunction with the associated graphics, respectively. If a participant reaches the “Finish” panel, a snippet of Handel’s *Halleluiah Chorus* is played. The sounds selected were chosen to provide participants with greater enjoyment and involvement in the game.

Section VI Research Development

Once study design concept was complete, research development required several phases that include writing the FIT application, submitting the project to the Institutional Review Board (IRB) for consideration and approval, seeking and gaining access to college students, and gathering study participants’ responses. The software application required approximately one year to write. Submission to the IRB and subsequent approval to conduct the research required one year. Requesting and receiving authorization to communicate with college students regarding the study required nine months. Data collection required approximately one year.

FIT was developed using MATLAB software. The product provides a number of advantages that include a robust *graphical user interface* (GUI), built in mathematical functions for data analysis, the capability of handling numerous matrices and is optimized for speed. The preponderance of code in FIT is written in native MATLAB. One of the six game panels in each of the nine content areas contains a video clip. Microsoft code is embedded in these panels to provide the necessary functionality to position, start, pause, and stop the videos. Recordings were made using the third party webcam product CyberLink YouCam. The videos were imported into the application. Each of the nine topic areas in FIT includes one of the six game panels with an audio clip. MATLAB built-in functions were used for recording and playback of the sound files. Many different graphics are displayed through the run of FIT. Images are a combination of pictures from Microsoft's Clip Art, Clip Art that has been edited or work created by the researcher. A variety of sound clips from Cosmi's 6000 Sound Effects are integrated into FIT such as applause, bells, cries, mouse clicks and sirens. Data is recorded only at the end of a complete and normal termination of the application. If an individual indicates in the demographics collection area of FIT that he or she is less than 18 years of age, a "Thank You" message is displayed that explains that it not possible to include his or her response at this time due to age restriction. The program terminates without saving demographics information.

FIT consists of a number of modules that participants move through in the application (Appendix H, Figure 11). The initial acceptance screen contains an explanation of the study and acts as a gate-keeper to allow access to individuals who are at least 18 years of age (Appendix B). FIT proceeds as described in the Research Design section. In brief, following the acceptance screen, participants are asked to provide demographic data; supply answers to

Survey 1 prior to an educational module; access material about *identity theft*; supply answers to Survey 2 following the educational module; and provide feedback about the FIT experience.

The Institutional Review Board (IRB) at Iowa State University (ISU) has oversight of this study, because it involves *human subject research*. Doug Jacobson, PhD is the Major Professor for the study. The National Institute of Health requires training for *human subject research*. This was completed. A copy of the certificate is available at the IRB office at ISU. As part of the application process, the IRB requires that copies of documents associated with the study be approved. The complete research application is available at the IRB office at ISU in Ames, Iowa. Copies of the documents used for communication in the study that include the Identity Theft Flyer, Recruitment Email, Invitation Script, and Informed Consent are available in this work (Appendix A). The FIT study was initially approved for a two year period ending July 9, 2016. It has subsequently been extended to continue through July 9, 2018.

CHAPTER 3

RESEARCH RESULTS

Section I Text-Based and Game-Based Results

Statistics for four hundred participants who completed sessions with FIT are reported. One hundred eighty received the text-based educational module (*tbm*). Two hundred twenty received the game-based educational module (*gbm*). Statistics compiled include the frequency of participants who received the two different educational modules with respect to demographics and feedback information; averages, standard deviations, minimums, maximums and correlations in relation to cumulative scores, demographic information, time and participant feedback; and participants' change in Survey 1 and Survey 2 responses. Appendices contain complete results. Descriptions of the appendices and tables as well as data contained in them follow.

The frequency of individuals who received the text-based and game-based educational modules is available (Appendix J). The data is reported with respect to the four demographic groups in Table 4 through Table 7. Table 4 reports the frequency of individuals by age group. Table 5 lists the frequency of individuals by gender. Table 6 contains the frequency of individuals by technology savviness level. Table 7 reports the frequency of individuals by education level.

Beginning with Appendix J Table 4 for the four age groups (18 – 22, 23 – 30, 31 – 45, and 46 and greater) the percent of participants who received *tbm* is 28%, 41%, 21% and 10%, respectively. For the same four groups the percent of participants who received the

gbm is 47%, 30%, 16% and 6%, respectively. Totals for the two different educational modules by age group are listed.

Appendix J Table 5 reports the gender of the participants. Females and males constituted 64% and 36% of the group of participants who received the *tbm*. In the case of participants who received the *gbm*, females and males made up 67% and 33% of this group. Totals for the two different educational modules by gender are included.

Appendix J Table 6 lists data for participants' self-assessment of their technology savviness (low, low to medium, medium, medium to high, high). The percents of participants who received the *tbm* are 9%, 18%, 30%, 32% and 11%. For participants who received the *gbm* percents for technology savviness are 5%, 24%, 36%, 26%, and 10%. Totals for the two different educational modules by technology savviness are listed.

Appendix J Table 7 provides information regarding five levels of education that participants' achieved (some high school, high school graduate, one year college, two years college, more than two years college). Participants who received the *tbm* stated education levels of 7%, 19%, 33%, 23% and 18%. For participants who received the *gbm* 9%, 22%, 33%, 19% and 17% reported academic achievement at these levels. Totals for the text-based and game-based modules by level of education are included.

Several appendices report relationships between participants' responses on Survey 1 and Survey 2 and areas such as time, demographics, and feedback. The point system described earlier was used to assess participants' changes in responses from Survey 1 to Survey 2. Cumulative scores were calculated by first determining a score for a participant's movement on a specific question. After scores were computed for the nine individual questions the values were added together to determine the cumulative score. This summary

score, hereafter referred to as the score, is used to assess statistics that include averages, standard deviations, minimums, maximums and correlations in relation to time, demographic information, and participant feedback. Results that examine score and time versus demographic information are available (Appendix K). In addition, comparisons of score and time to participant feedback are available (Appendix L).

Appendix K includes information that relates score, time and demographic information. It contains two sections Part I and Part II that contain five tables structured in the same format. Part I examines data for participants who received the *tbm*. Part II lists information for participants who received the *gbm*. Descriptions of Tables 8 through Table 12 and Table 13 through Table 17 follow for Part I and Part II.

Appendix K Part I Table 8 lists overall results for score and time of participants who received the *tbm*. Statistics include averages, standard deviations, minimums, maximums and correlation. The four tables that follow, Table 9 through Table 12, drill deeper to explore score in relation to demographics. For example, Table 9 examines score and time by age groups (18–22, 23–30, 31–45, 46 and greater). Standard deviations, minimums, maximums and correlations with respect to score and time are listed. Table 10 compares score and time by gender. Averages, standard deviations, minimums, maximums and correlations are included. The fourth table, Table 11, examines scores and time in relation to technology savviness groups (low, low to medium, medium, medium to high, high). Statistics reported include averages, standard deviations, minimums, maximums, and correlations. Table 12, the last table in Part I, provides statistics for score and time in relation to education level (some high school, high school graduate, one year college, two years college, more than two years college). Averages, standard deviations, minimums, maximums and correlations are

included. Part II Table 13 through Table 17 contains statistics for participants who received the *gbm*. They follow the same format.

Results in Appendix K show the average score for participants who received the *gbm* are greater than for participants who received the *tbm*. Table 8 and Table 13 are summary tables for participants who received text-based and game-based educational modules. The tables report average scores of 1.36 and 6.85 for the two groups. In addition, Table 8 and Table 13 list the average time in seconds participants remained in the text-based and game-based educational modules to be 527 and 1002. Participants who received the *gbm* remained in the application longer than those who received the *tbm*.

Appendix K includes other tables that can be compared such as Table 9 and Table 14 that report results by age group. Average scores for participants who received the *tbm* are 1.27, 1.59, 1.08, and 1.17. In the four age groups, average scores for participants who received the *gbm* are 7.63, 6.35, 5.89 and 6.00. Scores for participants who received the *gbm* are greater than for those who received the *tbm*. Also, the average times spent by participants who received the *gbm* are greater than for those who received the *tbm*.

Appendix K Tables 10 and 15 examine score and time by gender for the participants who received the *tbm* and the *gbm*, respectively. Results within the tables are similar for females and males. For example, average scores for females and males in Table 10 for participants who received the *tbm* are 1.36 and 1.34. Average scores in Table 17 for females and males who received the *gbm* are 6.88 and 6.78. Average times for females and males who received the *tbm* are 538 and 707. For females and males who received the *gbm* averages times are 1058 and 854. Scores for participants who received the *gbm* are greater

than those for those who received the *tbm*. In addition, the average times spent by participants who received the *gbm* are greater than for those who received the *tbm*.

Appendix K Tables 11 report 16 average scores and times in relation to technology savviness levels. Average scores for participants who received the *tbm* for the five levels are 1.06, 1.28, 1.41, 1.38, and 1.53. Average scores for participants who received the *gbm* are 7.20, 6.98, 6.73, 6.89, and 6.76. Average scores for participants who received the *gbm* are greater than for participants who received the *tbm*. Average times for participants who received the *tbm* are 562, 515, 546, 488, and 581. Average times for the group who received the *gbm* are 869, 1014, 899, 1063, and 1263. The average times participants remained in the *gbm* are greater than for those who received the *tbm*.

Appendix K Tables 13 and 17 report average scores and times by education level. Average scores for participants who received the *tbm* for the five levels are 1.15, 1.49, 1.17, 1.37, and 1.47. Average scores for participants who received the *gbm* are 5.81, 7.13, 7.66, 6.23, and 6.00. The average scores for participants who received the *gbm* is greater than for participants who received the *tbm*. The average times for participants who received the *tbm* are 672, 513, 503, 481 and 586. The average times for participants who received the *gbm* are 1079, 898, 971, 976, and 1200. The average times participants spent who received the *gbm* are greater than for participants who received the *tbm*.

Appendix L contains four sections that include Part I, Part II, Part III and Part IV. Results in these sections report participant feedback with respect to benefit and enjoyment levels as well as comments. Part I lists summary results in Tables 18 and 19. Part II and Part III follow the same format and contain four tables, Tables 20 through 23 and Tables 24 through 27. The tables report results for participants who received the *tbm* and *gbm*,

respectively. Part II and Par III report averages, standard deviations, minimums, maximums for scores and time by benefit level and enjoyment level. Part IV contains Figure 12 and Figure 13 that display score in relation to benefit and enjoyment levels.

Appendix L Part I Table 18 lists overall feedback with respect to five benefit levels (no opinion, none, low, moderate, high). Results for participants who received the *tbm* are 52%, 29%, 18%, 1%, and 0%. Results for individuals who received the *gbm* are 9%, 1%, 11%, 23%, and 57%. In the case of no opinion, 43% fewer indicated this response in the group that received the *gbm* than in the group that received the *tbm*. For the category of none, 28% fewer participants who received the *gbm* selected this option than those who received the *tbm*. In the third level of low, 7% fewer participants who received the *gbm* responded with this choice than those who received the *tbm*. For moderate 22% more participants who received the *gbm* selected this choice than for those who received the *tbm*. For the choice of high, 57% more participants who received the *gbm* indicated this option than for those who received the *tbm*.

Appendix L Part I Table 19 contains feedback from participants by enjoyment level (no opinion, none, low, moderate, high). Participants who received the *gbm* responded more favorably in the enjoyment feedback area than those who received the *tbm*. For individuals who received the *tbm* 31%, 11%, 49%, 8%, and 1% selected the five enjoyment levels. In the case of participants who received the *gbm*, 9%, 1%, 14%, 25%, and 53% indicated the five enjoyment levels. For no opinion, 22% fewer participants who received the *gbm* selected this category. For none, 10% fewer participants who received the *gbm* selected this choice. In the third area, low, 35% fewer participants who received the *gbm* selected this

option. For the moderate level, 17% more participants who received the *gbm* made this selection. In the level high, 52% more participants who received the *gbm* picked this choice.

Appendix L Part II and Part III contain participant information for those who received the *tbm* and *gbm*, respectively. Part I Table 20 examines overall results for benefit and enjoyment. Table 21 lists statistics for score and time in relation to five benefit levels (no opinion, none, low, medium, high). Table 22 presents statistics for score and time with respect to five enjoyment levels (no opinion, none, low, medium, high). Statistics reported for Tables 21 and 22 include averages, standard deviations, minimums, maximums, and correlations. Table 23 reports samples of participants' comments. Part III Tables 24 through 27 report results for participants who received the *gbm*.

Appendix L Part II Table 20 and Part III Table 24 show average benefit and average enjoyment are greater for participants who received the *gbm* than for those who received the *tbm*. Table 21 and Table 25 and Table 22 and Table 26 show the average scores for the benefit and enjoyment levels are higher for participants who received *gbm* than for those who received the *tbm*. For example in Table 21 and 25, for the benefit levels of no opinion, none, low, moderate and high average scores for participants who received text-based and game-based educational modules results are 1.31 and 5.90; 1.02 and 0.00; 1.97 and 8.13; 2.0 and 7.24; and NA and 6.66, respectively. Tables 22 and 26 report enjoyment levels of no opinion, none, low, moderate and high average scores for participants who received text-based and game-based educational modules of 1.20 and 6.37; 0.37 and 0.00; 1.58 and 7.87; 2.0 and 6.89; and 3.00 and 6.72, respectively. In addition, the average times spent by participants who received the *gbm* in relation to benefit and enjoyment levels are greater than for participants who received the *tbm*.

The frequency of participants' changes in responses for the nine survey questions is available (Appendix M). Tables 28 through 37 are included. Nine potential outcomes exist for each set of questions from Survey 1 and Survey 2. These are listed in Table 2.

Table 2: Possible Survey 1 and Survey 2 Responses

Survey 1	Survey 2
incorrect	incorrect
incorrect	don't know
incorrect	Correct
don't know	Incorrect
don't know	don't know
don't know	Correct
correct	Incorrect
correct	don't know
correct	correct

A participant's responses for a particular question determine one of the results in Table 2. The outcome is calculated for the nine questions individually and tallied for the two educational groups. The results reflect the change in responses on a given question per person, if it exists.

Appendix M Table 28 is a color-coded key that includes five shades of blue used to highlight significant differences between text-based and game-based values in entries of Table 29 through Table 37. Blue colors represent incorrect/incorrect, "don't know"/"don't know", incorrect/correct, "don't know"/correct, and incorrect/"don't know". Frequency data is reported for the nine questions in Table 29 through Table 37. For example, Table 29 lists frequency information for Question 1. Table 30 lists frequency information for Question 2 and so forth. Results for Table 29 through Table 37 show greater positive change for participants who received the *gbm* than for those who received the *tbm*.

For Appendix M Table 29 along the main diagonal the percents for incorrect/incorrect and “don’t know”/”don’t know” are lower for participants who received the *gbm* than for those who received the *tbm* module. This indicates that a greater percent of participants who received the *gbm* changed their response on the post-survey to move from either of these cases. Text-based and game-based results for incorrect/incorrect and “don’t know”/”don’t know” are 18% and 4%; and 28% and 1%, respectively.

Another indicator In Table 29 of better performance for participants who received the *gbm* are results in the far right column for incorrect/correct and “don’t know”/correct. For incorrect/correct the percent of participants who received the *tbm* and *gbm* are 2% and 24%. For “don’t know”/correct the results are 7% and 37%.

A third indicator of better performance in Table 29 for participants who received the *gbm* is in the lower left region of the table for correct/incorrect and correct/”don’t know”. Results for correct/incorrect for the text-based and game-based educational modules are 1% and 0%. Results show that participation in the *gbm* did not cause participants to move from a correct response in the pre-survey to and incorrect one in the post-survey. For correct/”don’t know” the percents for text- and game-based participants are 1% and 0%, respectively. This shows that participants who received the *gbm* did not change from a correct response.

Finally, results in the lower right-hand corner indicate the percent of correct/correct responses are similar for participants who received the text- and game-based educational modules at 31% and 27%, respectively. Neither educational module caused participants to change from a correct response.

Complete reports for Questions 2 through 9 are listed in Tables 30 through 37. Results along the main diagonal show no change for incorrect/incorrect and “don’t

know”/”don’t know” are lower for participants who received the *gbm*. For the majority of questions in the upper right corner for incorrect/”don’t know”, incorrect/correct and “don’t know”/correct results favor participants who received the *gbm*.

Exceptions in Appendix M include Table 20 and Table 32 for Questions 2 and 4 where results were better for participants who received the *tbm*. For Question 2 the incorrect/”don’t know” values are 9% and 6%. For Question 4 for incorrect/”don’t know” values are 19% and 11%. However, improvement in Questions 2 and 4 in the incorrect/correct category favors participants who received the *gbm*. Question 2 values for incorrect/correct are 7% and 26%. For Question 4 results for incorrect/correct are 4% and 14%.

Values in the lower left areas of Tables 30 through 37 report negative performance that include “don’t know”/incorrect, correct/incorrect, and correct/”don’t know”. These values are low for both groups. This means that learning modules did not cause participants to change their responses in the wrong direction.

Scores can be one of 37 possible values from -18 to 18. The total number of participants who received a score and the frequency are available as well as a graphical representation (Appendix N). Calculated scores in the Table 38 range between -5 and 16. Figure 14 represents the two sets of results plotted on one axis. Blue and red colors are used to indicate results for participants who received the text-based and game-based educational modules. The data in red is to the right of the data set in blue. This indicates that participants who received the *gbm* performed better on the individual questions.

Results for grouped questions examine the three focus areas of this research and include *lack of knowledge following an event, misconceptions prior to the occurrence of an*

event and *jargon* are available in Table 39 (Appendix O). Questions 1, 2 and 7; 3, 6, and 8; and Questions 4, 5, and 9 assess these areas, respectively. Table 39 contains two parts 39a and 39b. The former is the key for the latter. Three colors are used to highlight performance and include red to indicate worsening, yellow to represent no change, and green to relate improvement. The worsening column (Wor) contains averages for “don’t know”/incorrect, correct/”don’t know”, and correct/incorrect. The no change column (NC) lists the averages for incorrect/incorrect and “don’t know”/”don’t know”. The improvement column (Imp) includes averages for incorrect/”don’t know”, incorrect/correct, and “don’t know”/correct. The similar column (Sim) displays asterisks in rows that have averages that are close within the groups. In addition, in Appendix O Table 39 further examination is given to averages that consider initial correct responses with either incorrect or “don’t know” as well as correct. Results for the first two are combined in the red CI/CD column. The correct/correct (CC) column is displayed in green. Text-based and game-based grouped questions are presented on the left and right sides of Table 39b, respectively.

The premise that grouped questions address specific topics is confirmed in Table 39. For example, grouped Questions 1, 2 and 7 results are essentially the same for two of the three questions. Questions 1 and 2 results in the Imp, Wor and NC columns for both educational methods are similar. Also, the value in the worsen column for Question 7 is close to those of Questions 1 and 2 for both educational methods. There is no difference in the CI/CD and CC columns for Questions 1, 2, and 7 for the two educational strategies. For Questions 3, 6, and 8, Questions 3 and 8, behave the same for the text-based method. Also, the Wor column for Question 6 is aligned with Questions 3 and 8. For the game-based strategy, Questions 3, 6, and 8 behave the same for Imp, Wor and NC. There is no difference

in the results for CI/CD and CC for the two educational methods. For Questions 4, 5 and 9, Questions 5 and 9 behave the same for the text-based method. The Wor column for Question 4 is aligned with Questions 5 and 9. For the game-based method results for Imp, Wor and NC are the same. There is no difference between the text-based and game-based methods for CI/CD and CC. Results for the grouped questions in the improvement and no change columns favor the game-based method.

Appendix P contains data from this research. Sets of results from the text-based (Table 40) and game-based (Table 41) educational modules are located there. Included are values for age group, gender, technology savviness level, education level, responses for the pre- and post-surveys, time and scores.

Statistical tests (F-test and t-test) were done to compare time, benefit, enjoyment, and score results for text-based and game-based participants. In each of the four cases, the outcomes are statistically significant. They appear in the reports that follow. All of the results support game-based learning.

F-table for $\alpha = 0.05$ (source: http://www.socr.ucla.edu/Applets.dir/F_Table.html)

F-test for time

	<u>Game (1)</u>	<u>Text (2)</u>
n	220	180
d.f.	219	179
variance(var)	300,753.03	56,316.12

$$H_0: \delta_1^2 = \delta_2^2$$

$$H_1: \delta_1^2 \neq \delta_2^2$$

$$F_0 = (\text{game var})/(\text{game n})/(\text{text var})/(\text{text n})$$

$$= 4.369453025$$

$$\approx 4.37$$

For F(219,179) the d.f. are large and do not appear in the table, so use $F(\infty, \infty)$ which is 1.00.

$F_0 = 4.37$ is to the far right of the $F = 1.00$ in the red-shaded region of the graph. There is statistical evidence to reject $H_0: \delta_1^2 = \delta_2^2$ and for $H_1: \delta_1^2 \neq \delta_2^2$.

F-test for benefit

	<u>Game (1)</u>	<u>Text (2)</u>
n	220	180
degrees freedom (d.f.)	219	179
variance(var)	1.49	0.65

$$H_0: \delta_1^2 = \delta_2^2$$

$$H_1: \delta_1^2 \neq \delta_2^2$$

$$F_0 = (\text{game var})/(\text{game n})/(\text{text var})/(\text{text n})$$

$$= 1.870577067$$

$$\approx 1.87$$

For F(219,179) the d.f. are large and do not appear in the table, so use $F(\infty, \infty)$ which is 1.00.

$F_0 = 1.12$ is to the right of the $F = 1.00$ in the red-shaded region of the graph. There is statistical evidence to reject $H_0: \delta_1^2 = \delta_2^2$ and $H_1: \delta_1^2 \neq \delta_2^2$.

F-test for enjoyment

	<u>Game (1)</u>	<u>Text (2)</u>
n	220	180
d.f.	219	179
variance(var)	1.45	1.06

$$H_0: \delta_1^2 = \delta_2^2$$

$$H_1: \delta_1^2 \neq \delta_2^2$$

$$\begin{aligned} F_0 &= (\text{game var})/(\text{game n})/(\text{text var})/(\text{text n}) \\ &= 1.11933767635 \\ &\approx 1.12 \end{aligned}$$

For $F(219,179)$ the d.f. are large and do not appear in the table, so use $F(\infty,\infty)$ which is 1.00.

$F_0 = 1.12$ is to the right of the $F = 1.00$ in the red-shaded region of the graph. There is statistical evidence to reject $H_0: \delta_1^2 = \delta_2^2$ and for $H_1: \delta_1^2 \neq \delta_2^2$.

F-test for score

	<u>Game (1)</u>	<u>Text (2)</u>
n	220	180
degrees freedom (d.f.)	219	179
variance(var)	11.96	1.97

$$H_0: \delta_1^2 = \delta_2^2$$

$$H_1: \delta_1^2 \neq \delta_2^2$$

$$\begin{aligned} F_0 &= (\text{game var})/(\text{game n})/(\text{text var})/(\text{text n}) \\ &= 4.958795285 \\ &\approx 4.96 \end{aligned}$$

For $F(219,179)$ the d.f. are large and do not appear in the table, so use $F(\infty,\infty)$ which is 1.00.

$F_0 = 4.96$ is to the far right of the $F = 1.00$ in the red-shaded region of the graph. There is statistical evidence to reject a $H_0: \delta_1^2 = \delta_2^2$ and $H_1: \delta_1^2 \neq \delta_2^2$.

t-table for $\alpha = 0.05$ (source: <http://www.socr.ucla.edu/applets.dir/t-table.html>)

t-test for time

	<u>Game (1)</u>	<u>Text (2)</u>
n	220	180
d.f.	219	179

$$H_0: \mu_1 = \mu_2$$

$$H_1: \mu_1 > \mu_2$$

$$\text{degrees freedom (d.f.)} = n_1 + n_2 - 2 = 398$$

$$t \text{ with d.f. of } 398 = 11.58$$

$$\approx 11.58$$

This is the critical value from the t-table. For large d.f. (∞) the value from the t-table is 1.645.

Since the calculated value is beyond this, there is statistical evidence to reject

$$H_0: \mu_1 = \mu_2 \text{ and for } H_1: \mu_1 > \mu_2.$$

t-test for benefit

	<u>Game (1)</u>	<u>Text (2)</u>
n	220	180
d.f.	219	179

$$H_0: \mu_1 = \mu_2$$

$$H_1: \mu_1 > \mu_2$$

$$\text{degrees freedom (d.f.)} = n_1 + n_2 - 2 = 398$$

$$t \text{ with d.f. of } 398 = 24.41673829$$

$$\approx 24.42$$

This is the critical value from the t-table. For large d.f. (∞) the value from the t-table is 1.645.

Since the calculated value is beyond this, there is statistical evidence to reject

$$H_0: \mu_1 = \mu_2 \text{ and for } H_1: \mu_1 > \mu_2.$$

t-test for enjoyment

	<u>Game (1)</u>	<u>Text (2)</u>
n	220	180
d.f.	219	179

$$H_0: \mu_1 = \mu_2$$

$$H_1: \mu_1 > \mu_2$$

$$\text{degrees freedom (d.f.)} = n_1 + n_2 - 2 = 398$$

$$t \text{ with d.f. of } 398 = 15.71.643676$$

$$\approx 15.72$$

This is the critical value from the t-table. For large d.f. (∞) the value from the t-table is 1.645.

Since the calculated value is beyond this, there is statistical evidence to reject

$$H_0: \mu_1 = \mu_2 \text{ and for } H_1: \mu_1 > \mu_2.$$

t-test for score

	<u>Game (1)</u>	<u>Text (2)</u>
n	220	180
d.f.	219	179

$$H_0: \mu_1 = \mu_2$$

$$H_1: \mu_1 > \mu_2$$

$$\text{degrees freedom (d.f.)} = n_1 + n_2 - 2 = 398$$

$$t \text{ with d.f. of } 398 = 21.51437762$$

$$\approx 21.51$$

This is the critical value. For large d.f. (∞) the value from the t-table is 1.645.

Since the calculated value is beyond this, there is statistical evidence to reject

$$H_0: \mu_1 = \mu_2 \text{ and for } H_1: \mu_1 > \mu_2.$$

CHAPTER 4

SUMMARY AND CONCLUSIONS

Summary

Fraud perpetrated by *identity theft* consumes billions of dollars annually in the United States alone. It affects trust through all walks of society, crippling systems at the corporate as well as individual levels. Government, financial institutions, retail enterprises, insurance networks and medical facilities, to name a few, suffer from the burden of tremendous losses that are the result of fraudulent transactions.

At the individual level *identity theft* can be devastating. Financial consequences represent a significant problem, since related credit issues can haunt the victim for years. The loss of insurance benefits can jeopardize well-being and other services. In addition, significant quantities of resources of time and funds are needed to unravel and clear long-lasting and troubling consequences.

Public awareness about *identity theft* has improved in recent years, but more work is needed. Federal programs to inform citizens include websites, television commercials or pamphlets distributed via the United States postal system. Security products are designed to protect individuals from *identity theft* and to assist with the fallout following an attack. Greater and more extensive coverage by the news media have provided necessary information. However, the crime continues to grow with the number of victims increasing. This is particularly true when considering the unfortunate outcomes of misinformed individuals who, as a result of making poor choices, place themselves at risk. The inconceivable and unconscionable consequences that result from insider abuses is cause for alarm. The path forward is dire. Creative solutions are essential to mitigate *identity theft*.

Fraudulent methods to steal *identities* and then use them to commit crimes are diverse. A host of these schemes focus on non-technical means. *Social engineering* is one such strategy that is resilient, productive and simple to implement. To a large extent to be successful, these *frauds* depend on an unsuspecting and uninformed pool of potential victims. To combat attacks that exploit social vulnerabilities at the individual level, better awareness of the crime that can lead to behavior change is necessary. While the threat of insider events, such as the recent Wells Fargo debacle, remain out of the scope of the general citizenry to deter. Issues the individual can address need to be secured. Greater and more effective *identity theft* education is critical to supply the public with the information required to avoid becoming a victim. The adage “An ounce of prevention is worth a pound of cure” is appropriate. In truth, with the advent of mobile devices such as smart phones, *identity theft* education should begin when children are very young in order to establish good habits. Because of the abuse by *identity thieves* of young adults and of Federal research guidelines, the focus of this study is college students.

Contemporary research in learning theory and education suggests that digital game-based learning is effective. Work is evolving as applications are developed to address a wide variety of content areas. Current development in game-based learning targets material outside the sphere of cyber security. Few exceptions exist. In particular, game-based learning has not been applied to educate the public about *identity theft*.

Conclusions

This study examined and compared results for two different educational delivery methods, one text-based the other game-based. Three over-arching areas that contribute to *identity theft* were considered that include an individual’s lack of knowledge of the

consequences following an event, prior misconceptions before the occurrence of an event, and jargon. Statistics for the three sets of grouped questions, 127, 368, and 459, favor participants who received the *gbm*. Results reported individually for the nine survey questions and on participant feedback for benefit and enjoyment are higher for the game-based group than for their text-based counterparts. In addition, the average time spent by participants who received the *gbm* is greater than for participants who received the *tbm*. Because information is the same, it suggests that the *gbm* held participants' interest longer than the *tbm*. Higher scores, greater benefit and enjoyment levels, and more time in the *gbm* support game-based learning as an alternative to existing methods. The purpose of FIT is not to replace resources that are currently available to inform the public, but rather to complement these strategies.

As evidenced in the statistical analysis outlined in the Research Results section of this document, there exist significant differences in the outcomes between the text- and game-based participants. Scores, time, benefit and enjoyment levels are all greater for the game-based group. Of these four items, values for benefit and enjoyment are subjective results provided by the participant and then recorded. They directly reflect the individual's personal experience with FIT. The marked difference in these metrics for the two groups shows participants' greater level of satisfaction with the game-based learning module. This consequence leads to the question, "What is/are the reason(s) for the better benefit and enjoyment scores for these participants?" My thoughts on this question are outlined in the paragraphs that follow.

Significantly higher scores for participants who received the game-based educational module reflect greater understanding of the material addressed on the pre- and post-surveys.

This implies that the game-based group was more prepared to answer questions correctly on the post-survey. The result suggests the question, “Why do game-based participants perform better?” A higher level of interest in the game-side of FIT is a possible explanation. This is reflected in the significantly greater length of time that participants remained in the game-side of FIT, nearly twice the duration of their text-based group counterparts. A logical next question is, “Why do participants continue in the game-side of FIT longer?” One possible answer, that they are more satisfied with the game-side experience, circles back to benefit and enjoyment. This is the same process that Mihaly Csikszentmihalyi purports and occurs in *flow*. The result is that a player is drawn deeper into the experience on various levels and *wants* to continue the activity, in this case learning about *identity theft*.

Examining details more closely, recall that identical content is included in the two learning modules, but presented in substantially different ways. Individual Q & A panels are most closely related to their text-based counterparts. In the case of the game-side, one paragraph of text relates a single topic and is displayed on a panel rather than on the text-side where six paragraphs are visible on a screen. Reading is required in both instances, but the game-side focuses on one issue. The related question addresses that particular content. The game-based environment affords the participant immediate feedback after a question is answered. Learning is checked instantly and rewarded with points and cheerful sounds when the correct responses are provided.

Returning to the game-side, the level of activity required is greater than for the text-based content areas. Minimally, a pick from one of the three possible choices is required prior to moving forward in the game. In addition, the “Next” button must be clicked on every panel in order to proceed. These actions mandate a level of player participation on

every panel that contains an *identity theft* clue whether it is text, audio, video or a puzzle. This degree of interaction and engagement is not required for the material on the text-based panels. In this case, the participant selects a screen to view and closes it when he or she decides to leave the page.

The appealing and *fun* aspects of the game-side are relevant. Inviting colors, graphics, sounds and the game-environment are positive factors. They provide the participant with a multi-sensory experience that addresses different learning styles. They engage the participant on a variety of levels. This, in turn, promotes interest that requires the participant to spend a greater length of time to explore the environment. Consequently, the higher level of involvement supports curiosity, understanding and learning about *identity theft* information. This leads to better performance on the pre- and post-surveys that is demonstrated and recorded in the scores.

The game-based learning readings included in the References section of this document are reflected in the research. For example, Marc Prensky discusses games in *Fun, Play, and Games: What Makes Games Engaging*. He addresses 12 points that foster learning. Several items illustrate the connection. Prensky includes *fun* and how it is related to *enjoyment* and *pleasure*. Similarly, he includes *play* and its relationship to *involvement*. Some of the other elements that Prensky discusses are *goals* and how they promote *motivation* and *outcomes* and *feedback* that support learning. These items, as well as others outlined in the article, are integrated into FIT. They form a framework that encourages interest and engagement that provides a positive and supportive learning environment. Results are reflected in the higher scores for game-based participants on the pre- and post-surveys.

Another example of game-based learning theory integrated into FIT is addressed in *Intrinsic Motivation and Effective Teaching* by Mihaly Csikszentmihalyi. His work addresses internal motivation, an integral component for success in games. The interactive nature of FIT, rewards for correct responses, and the continuing challenges afford each participant with a unique and diverse learning experience. *Flow* is impacted by the variety of content on the game-based panels. Participants *want* to be successful. Positive reinforcement promotes skill, which, in turn, supports satisfaction and a desire for greater challenges. This circular relationship may, in part, explain the significantly longer period of time that game-based participants remain in FIT. More time in the learning module equates to a greater opportunity to learn about *identity theft*. Consequently, this promotes the participant's greater sense of benefit and enjoyment with the game-side of FIT.

The article *Games, Learning and Assessment* by Valerie J. Shute and Fengfeng Ke discusses the importance of substantive measurement tools. The development of a suitable metric is imperative. The scoring system designed for and implemented in FIT represents a fundamental component of the assessment process. Measurement of learning is integrated into the application. Higher scores for game-based participants, determined by the results on the pre- and post-surveys, reflect greater understanding of the material.

Other readings that directly relate to the better performance for game-based participants in FIT include *Benefits of Playing Video Game* by Isabela Granic, Adam Lobeland Ruger C.M.E. Engels and *Why Educators Should Care about Games* by Sasha A. Barab, Melissa Gresalfi, and Anna Arici. These articles stress the importance of engagement and motivation in the learning process. In particular, they examine games in the context of

the digital world. Elements under consideration are embedded into FIT and appear to contribute to the higher scores observed for the game-based participants.

In the article *The Interplay of Game Elements with Psychometric Qualities, Learning, and Enjoyment in Game-Based Assessment* by Yoon Jeon Kim and Valerie J. Shute, the authors address the issue of *linearity* in game sequences. The term *linearity* is used to refer to specific paths that must be followed in the game environment. *Linearity* constrains free-choice and limits decision making, fundamental concepts necessary for creative thinking and problem solving. The effect on assessment in relation to enjoyment, fairness, learning, reliability and validity are discussed in the article. *Linearity* was addressed in the design of FIT, because it was avoided. Participants are able to choose to explore any of the nine different content areas in any order from the Main Game Board panel. In addition, experience differs from participant to participant, since clue and question panels are displayed randomly. The inclusion of *non-linearity* in the initial design process of FIT creates a fresh and new experience for each participant. This, in turn, supports enjoyment, fairness, learning, reliability and validity in assessment component. These elements support the higher scores observed for game-based participants.

Matthew Gaydos discusses game-based learning in *Seriously Considering Design in Educational Games*. He focuses on the design of the game prior to its development as an integral element of its success as an educational tool. He urges that initially projects be well-defined in order to achieve their respective goals. Gaydos' recommendations are reflected in FIT. The application was conceived in its existing form. The basic structure of FIT was determined from the beginning and is reflected in the flow chart (Appendix H). Nine content areas were set. Material to address these topics was assembled. Arrangement of a

three by three grouping of game icons for the Main Game Board was determined early in the design phase. In addition, placement of the other information that appears on the Main Game Board was established in the initial stages of development. The variety of fonts, colors, graphics, sounds, text, audio and video information, and puzzles were a part of the original concept of FIT. Decisions to incorporate these elements were made for the sole purpose of promoting engagement in learning about *identity theft*. Evidence of the efficacy is observed in the significantly better performance of the game-based participants.

One thing that should be noted is that the score of zero on a particular set of pre- and post-survey questions indicates no change. This indicates that exposure to the application had no effect on the participant, since the individual did not change his or her response. Depending on the circumstance, this can be interpreted in more than one way. In the cases of incorrect/incorrect or “don’t know”/”don’t know” the score of zero indicates no change. On the other hand, for a person who responds correctly on the pre- and post- surveys the score of zero is positive outcome, since the application did not cause the individual to make an error.

Future directions with this project include two tracks. One focuses on continuing research in this area with updated releases of the application. New threats arrive on the scene. Existing pervasive threats are of concern as well. Research in the area of cyber security education in conjunction with game-based learning is in its initial stage.

The other direction is to separate the game element of the application for use exclusively as an educational tool. On this path FIT can develop and evolve to meet the challenges of better *identity theft* education outside of the constraints of research. As a free-standing educational game, the application might be able to assist young audiences that are

difficult to reach, because of existing research guidelines. Interest exists in both of these directions. Perhaps they are not mutually exclusive.

During the process of development, implementation and analysis for this research several items became aware to me. Some are ideas that I thought of, while other are suggestions made by participants and colleagues. They provide a substantial pool of directions to pursue for future research. Discussions of a number of possible ways that FIT can be improved, enhanced and evolve are considered in the following paragraphs.

Participants offered several noteworthy ideas for future releases of FIT. Included in their suggestions is that the player be allowed to select the questions that they want to answer rather than the current random sequence within each of the nine content areas. The initial design decision to randomize the question display was to provide variety in the experience so that no two players would have identical scenarios. Given the interest in FIT, the idea of allowing participants to select the tasks is worth exploring. Current research in game-based learning theory supports this position.

A number of participants expressed regret in being unable to “finish the game”, because of prior time commitments. The suggestion was made that FIT be able to accommodate people who need to leave, but could return at a later time to continue play. Exit and resume functionality could be implemented in FIT, but was not considered in the initial design phase of the project. It is clear that the game aspect of FIT played a role in the level of interest participants expressed. The importance of a greater awareness of *identity theft* and the need for better education in this area suggest that the desire to be successful in FIT is a good motivating factor in holding people’s interest. This recommendation is worth considering.

Another item that was suggested in the feedback comments section of FIT is to allow players to redo questions that they answer incorrectly. From the research perspective this was not considered so that empirical data could be recorded. However, from a learning theory perspective this idea has merit, since the purpose of FIT is to educate players about *identity theft*. This focus parallels non-educational games that are created for entertainment and adds another layer to assist in learning content.

A possible modification to assess in FIT is the addition of a greater number of higher point questions. Currently, three of six questions in each of the nine topic areas are a one point questions. In the initial project design, consideration of point value concerned and was focused on the type of question. For example, a panel with an audio clue that requires listening is weighted more heavily than one that includes several lines of text to read. It is worth examining the idea of whether to increase the existing point values so that there are fewer single point questions or to replace some text questions that require reading with other formats that have higher point counts.

Input from colleagues addressed the need for *identity theft* education at both ends of the age spectrum. I received requests from co-workers to develop FIT for children in grade school. When I explained the Federal research constraints, the response that I received was that children need this information. At the other end of the age spectrum, I received recommendations that a senior version of FIT be developed, because so many are targeted by *fraudsters*. There exists significant interest in *identity theft* game-based learning to benefit different age groups.

As I worked on this project, a variety of things occurred to me that might be worth investigating in the future. One of these items is to develop a robust game narrative to

enhance the FIT experience. For example, instead of a brief description of the research project at the start of the application something more compelling could be developed such as having a player assume the role of an investigator or of a cyber-crime specialist in order to gather information about *identity theft*. The nine topic areas that contain six questions could be expanded so that content areas are woven together. For example, the Home area could include detail about the physical surroundings or patterns of events that transpire through the day. Or perhaps, the focus could be on elaborating on vulnerabilities within specific areas of the home where the player moves during the game such as phones, computers, trash bins and other resources frequented by *identity thieves*. Many potential directions exist to examine in future development of a substantive game narrative.

A possible way to affect the length of the game is to have fewer topic areas and/or limit the number of questions within these areas. This could be a benefit. For example, from the standpoint of addressing the length of time that is required to complete the game, fewer questions are needed. Along the same track, content could be designed to target particular problems. Currently, FIT exists as a multifaceted educational tool. Perhaps smaller modules designed to target specific issues is a direction to consider. Multiple related game questions and content could be useful and worthwhile. This option has another advantage in that the entire large FIT program would not need to be updated. The smaller modules would be more nimble and easier to maintain to keep current. .

Additional internal games similar to the word search puzzles currently deployed in FIT could be created for the dual purposes of providing clue information and increasing motivation. Many types of small games could be adapted such as sudokus, crosswords, magic squares and others to pique interest and be added to the game panels. The small

embedded games would not consume a substantial amount of time. In terms of learning theory, they could provide extensions to the main task, a deeper understanding of the material to be learned, or build confidence in the player's ability to be successful. Several participants commented that they enjoyed the word search puzzles. Returning to learning theory, motivation is directly related to enjoyment. Factors that contribute to enjoyment represent an asset.

Expanding the application for a larger or perhaps more diverse audience is another possible direction. In this case, the issue becomes, "Can FIT become too big and unwieldy?" Material for particular demographic groups could be included. For example, in the case of the elderly, *identity theft* material relevant to issues that they experience could be developed and added. If a wave of a specific type of *fraud* is wreaking havoc on a particular group of people or region, incorporating this content into FIT could be done. Related to this idea is the possibility of designing FIT in such a way as to allow access to certain areas of the application. In other words, it might be useful to include pools of questions that focus on specific content areas. Rather than having six questions that relate to scams that can occur at the office, perhaps several times that number would be appropriate. The software could be designed to randomly select a specified number of questions from a pool. For example, rather than affording players a large array of choices to pursue, "turning on" certain material may be an option. In this case the idea is along the lines of "plug and play". Another related direction is to expand the software to select progressively harder questions from the pool as participants continue to be successful and to reverse course, if necessary. This issue returns to the question of whether FIT should house a comprehensive assortment of content or be a collection of smaller programs.

Deployment over the Internet is another way to extend FIT's impact to a greater audience. Technical issues that occurred during the development phase prevented a web interface application from being created so that FIT could be accessed via the Internet. This direction and opportunity requires additional investigation. As a web-based application FIT could reach countless people and provide a needed benefit to combat *identity theft*.

In considering the possibility of future research comparing text-based and game-based learning, it might prove useful to include additional questions on the demographics panel. Some items to add might be the most frequently used mode of transportation, average hours away from the residence, average weekly distance travelled, expanded age groups in both directions, as well as others. In addition, in light of the National conversation about LGBT issues, it might be necessary to subdivide the gender category. The demographics included in the current version of FIT showed little differences within the two groups of participants. The inclusion of additional demographics might confirm this finding or show that other factors can contribute to *identity theft*.

Further investigation of time is another possible area to consider in future research. Additions to FIT software would make it possible to track the length of time spent on every panel in the software. Another consideration is whether to separate the nine survey questions onto individual panels to facilitate the collection of time a participant spends on a given question. While the average time spent may be skewed by an individual who gets up and leaves the computer for a period of time, the information could provide a baseline to determine if some questions appear to be more challenging than others.

Recording the number of times a participant activates an audio or video clue might be of interest. It is possible for points to be awarded dependent on the number of times a

resource is accessed. For example, it could provide an incentive for players to carefully listen or observe from the beginning of the resource. The option to adjust the point count dependent on the number of times that information is accessed could be designed as a switch so that the player could turn it on or off.

The current version of the application provides participants with three choices for responses on the survey questions and to the game questions that include true, false and “don’t know”. A possible direction to expand the response options is to include a method to record the confidence level for the “don’t know” category. This could be implemented with a slide bar widget that would allow participants to indicate a level of assurance in a decision. For example, an individual could state a specific amount such as 85% on the confidence scale. Another person on the same question might select a value of 30%. This data would provide investigators with more information about how participants perceive a particular question.

A longitudinal study that tracks performance over time is a project to consider. This could address whether learning material in a game over short time can affect an individual over a longer period. At what age to begin a longitudinal study and for what length of time to continue are two items to consider. Examining results over an extended period could provide useful information relevant to combating *identity theft*.

In conclusion, this research showed that participants who received the *identity theft gbm* performed better than those who received the *tbm* in all three focus areas of this investigation. The importance of developing viable means to mitigate *identity theft* cannot be understated. Losses affect the individual and society as a whole on an epic scale. The related crimes are only getting worse. It is imperative that the arsenal of tools to fight

identity theft be extended in new directions to address this growing threat. FIT has showed that game-based learning in this area to be effective. Future work must be done in creative ways to expand the dissemination of information regarding the collection of related *frauds*. Further developments along this and other related lines are needed. FIT is a place to begin.

REFERENCES

- [1] *A Real Steal*, State Legislatures. Dec 2010, Vol. 36 Issue 10, pp 10, ISSN 01476041
- [2] *A Survey of Privacy and Security Issues in Social Networks*, Dolvara Gunatilaka, November 28, 2011, <http://www.cse.wustl.edu/~jain/cse571-11/ftp/social/>, retrieved August 30, 2016
- [3] F. Abagnale with S. Redding, *Catch Me If You Can*, Broadway Books, a division of Random House, Inc., 1980
- [4] F. Abagnale, *The Art of the Steal*, Broadway Books, a division of Random House, Inc., 2001
- [5] R. Abelson, M. Goldstein, *Millions of Anthem Customers Targeted in Cyberattack*, New York Times, February 5, 2015, <http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html>, retrieved August 6, 2016
- [6] A. Acquisti, *Privacy in Electronic Commerce and the Economics of Immediate Gratification*, EC' 04 May 17-20, 2004, ACM 1-58113-711-0/04/0005
- [7] Anti-Phishing Working Group, *Phishing Activity Trends Report 1st – 3rd Quarters 2015*, http://docs.apwg.org/reports/apwg_trends_report_q1-q3_2015.pdf
- [8] Anti-Phishing Working Group, *Phishing Activity Trends Report 4th 1 Quarter 2015*, http://docs.apwg.org/reports/apwg_trends_report_q4_2015.pdf
- [9] Anti-Phishing Working Group, *Phishing Activity Trends Report 1st Quarter 2016*, https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf
- [10] S. Baase, *A Gift of Fire: Social, Legal, and Ethical Issues for Computing and the Internet, 3rd Edition*, Pearson Prentice Hall, 2008
- [11] S. A. Barab, M. Gresalfi, and A. Arici, *Why Educators Should Care About Games*, Educational Leadership, September 2009, Vol. 67, No. 1 pp 76 – 80.
- [12] *Barak Obama's Passport Details Shared in Privacy Mix-up: Report*, March 30, 2015, <http://www.nbcnews.com/news/us-news/obamas-personal-details-shared-privacy-mix-report-n332401>, retrieved August 30, 2016
- [13] S. Barzilai, I. Blau, *Scaffolding Game-based Learning: Impact on Learning Achievements, Perceived Learning, and Game Experiences*, Computers and Education, Vol. 70, 2014, pp 65 – 79, 0360-1315/2013 Elsevier, Ltd.
- [14] BBC News, *Grandmother Robbed by Card Conmen*, 04/21/2008, http://news.bbc.co.uk/1/hi/scotland/edinburgh_and_east/7359067.stm

- [15] BBC News, *Net Card Fraud “Underestimated”*, 04/23/2008, <http://news.bbc.co.uk/1/hi/business/7362055.stm>
- [16] BBC News, *The Web Trade in Credit Card Details*, Anna Adams, 04/23/2008, <http://news.bbc.co.uk/1/hi/uk/7351100.stm>
- [17] R. L. Bednar, S. R. Peterson, *Self-Esteem: Paradox and Innovations in Clinical Theory and Practice*, American Psychological Association (APA) (1977), ASIN: B01K17KJ2U
- [18] F. Bellotti, B. Kapralos, K. Lee, P. Moreno-Ger, and R. Berta, *Assessment in and of Serious Games: An Overview*, Hindawi Publishing Corporation, *Advances in Human Computer Interaction*, Vol. 2013, Article ID 136864, pp 1 – 11
- [19] M. L. Benson, *Offenders or Opportunities: Approaches to Controlling Identity Theft*, *Criminology & Public Policy*, May2009, Vol. 8 Issue 2, pp 231 - 236
- [20] H. Berghel, *Fungible Credentials and Next-Generation Fraud*, *Communications of the ACM*, December 2006, Vol. 49, No. 12
- [21] H. Berghel, *Identity Theft, Social Security Numbers, and the Web*, *Communications of the ACM*, February 2000, Vol. 43, No. 2
- [22] H. Berghel, *The Two Sides of ROI: Return on Investment vs. Risk of Incarceration*, *Communications of the ACM*, April 2005, Vol. 48, No.4
- [23] A. Bhargav-Spantzel, A. Squicciarini and E. Bertino, *Privacy Preserving Multi-Factor Authentication with Biometrics*, DIM '06, November 3, 2006, ACM 1-59593-547-9/06/0011
- [24] E. Blakemore, *Report the Microsoft phone scam*, June 13, 2011, <http://blogs.microsoft.com/microsoftsecure/2011/06/13/report-the-microsoft-phone-scam/>, retrieved August 8, 2016
- [25] K. Blanchard and A. Cheska, *The Anthropology of Sport: An Introduction*, Praeger, September 30, 1984, ASIN: B001EQ62ZG
- [26] C. Bødker, *Jordsang: Digte*, Gyldendal,1991, ISBN-10: 8700073431, ISBN-13: 978-8700073432
- [27] R. Bose, *Intelligent Technologies for Managing Fraud and Identity Theft*, *Proceeding of the Third International Conference on Information Technology: New Generations (ITNG'06)*, IEEE 0-7695-2497-4/06
- [28] S. W. Brenner, *U.S. Cybercrime Law: Defining Offences*, *Information Systems Frontiers* 6:2,115-132, 2004 Kluwer Academic Publishers

- [29] R. G. Brody, E. Mulig, V. Kimball, *Phishing, pharming and identity theft* Academy of Accounting and Financial Studies Journal. Sept, 2007, Vol. 11 Issue 3, pp 43 – 57
- [30] G. Brown *Minds, Brains, and Machines (Mind Matters)*, Palgrave Macmillan, June 1989, ISBN-10: 0312031440, ISBN-13: 978-0312031442
- [31] C. Burkhalter, J. Crittenden, *Professional Identity Theft: What Is It? How Are We Contributing To It? What Can We Do To Stop It?*, Contemporary Issues in Communication Science & Disorders (CONTEMP ISSUES COMMUN SCI DISORD), Spring 2009, Vol. 36, pp 89 - 94, ISSN 1092-5171
- [32] F. Cassim, *Protecting Personal Information in the Era of Identity Theft: Just How Safe is Our Personal Information from Identity Thieves?*, ISSN 1727-3781, PER: Potchefstroomse Elektroniese Regsblad, 18(2):pp 69 - 110
<http://dx.doi.org/10.4314/pej.v18i2.02>, Retrieved July 14, 2016
- [33] M-T Cheng, H-C She, and L.A. Annetta, *Game Immersion Experience: Its Hierarchical Structure and Impact on Game-based Science Learning*, Journal of Computer Assisted Learning, June 2015, Vol. 31 Issue 3, pp 232 – 253
- [34] A. Combs, Ed., M. Germiné, Ed., B. Goertzel, Ed., *Mind in Time: The Dynamics of Thought, Reality, and Consciousness (Advances in Systems Theory, Complexity, and the Human Sciences)*, Hampton Pr, December 2003, ISBN-10: 1572732563, ISBN-13: 978-1572732568
- [35] M. Csikszentmihalyi, Applications of Flow in Human Development and Education, *Chapter 8: Intrinsic Motivation and Effective Teaching*, 2014 Springer Science & Business Media Dordrecht, DOI: 10.1007/978-94-017-9094-9_8, pp 173 – 187
- [36] M. Csikszentmihalyi, *The Psychology of Optimal Experience*, Harper & Row; 1st Ed., March 1990, ASIN: B010EV0KHW
- [37] K. Collins, *Here's What Your Stolen Identity Goes for on the Internet's Black Market*, July 23, 2015, <http://qz.com/460482/heres-what-your-stolen-identity-goes-for-on-the-internets-black-market/>, retrieved August 8, 2016
- [38] *Credit Reports and Scores*, <https://www.usa.gov/credit-reports>, retrieved August 29, 2016
- [39] S. Delaitre, *Risk Management approach on identity theft in biometric systems context*, Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), IEEE 0-7695-2567-9/06
- [40] *Deter, Detect, Defend, Avoid Theft*, https://www.in.gov/isp/files/Avoid_ID_Theft_Deter_Detect_Defend.pdf, Retrieved July 14, 2016

[41] R. Dhamija, J. D. Tygar, M. Hearst, *Why Phishing Works*, CHI 2006, April 22-27, 2006, ACM 1- 59593-178-3/06/0004

[42] T. Dinev, *Why Spoofing is Serious Internet Fraud*, Communications of the ACM, October 2006, Vol. 49, No. 10

[43] *DNC hack: What you need to know*, Tal Kopan, June 21, 2016, <http://www.cnn.com/2016/06/21/politics/dnc-hack-russians-guccifer-claims/index.html>, retrieved August 31, 2016

[44] J. S. Downs, M. B. Holbrook, and L. F. Cranor, *Decision Strategies and Susceptibility to Phishing*, Symposium On Usable Privacy and Security (SOUPS), July 12-14, 2006

[45] M. Egan, *Wells Fargo Scandal: Elizabeth Warren Wants Answers*, September 12, 2016, <http://money.cnn.com/2016/09/12/investing/wells-fargo-hearing-senate-ceo-testify-elizabeth-warren/index.html>, retrieved September 12, 2016

[46] C. Emami, R. Brown and R. G. Smith, *Use and acceptance of biometric technologies among victims of identity crime and misuse in Australia*, Trends and Issues in Crime and Criminal Justice, No. 511, Apr 2016: 1-6, ISSN:1836-2206

[47] S. Engelmann, T.W. Wood, Ed., *Engelmann's Direct Instruction: Selected Writings From the Past Half Century*, NIFDI Press, 1964, ASIN: B00OQU10WC

[48] P. A. Ertmer, C. Hmelo-Silver, Ed., A. Walker, Ed., H. Leary, Ed. *Essential Readings in Problem-Based Learning: Exploring and Extending the Legacy of Howard S. Barrows*, Purdue University Press, January 15, 2015, ISBN-10: 1557536821, ISBN-13: 978-1557536822

[49] Equifax, http://www.equifax.com/equifaxcomplete/Credit-Reports/?CID=3&credit_report_for_all_three_bureaus_M_E&adID=31032586442&DS3_KID=43700009807066765&gclid=CPGI7o-5584CFYbZMgodmfMGmg&gclsrc=ds, retrieved August 29, 2016

[50] *Expanding Service to Reach Victims of Identity Theft and Financial Fraud*, October 2010, http://www.ovc.gov/pubs/ID_theft/idtheftlaws.html, retrieved August 28, 2016

[51] Experian, http://www.experian.com/credit-report-partner/index-y.html?sc=678648&bcd=ad_c_sem_427_31675184170&k_id=20b18941-a8c6-4f60-a263-e5898b7b5cb6&k_kw=credit%20reports%20all%20three%20bureaus&k_mt=e&pc=sem_exp_yahoo&cc=sem_exp_yahoo_ad_346071568_8919817543_31675184170_credit%20reports%20all%20three%20bureaus_e__20b18941-a8c6-4f60-a263-e5898b7b5cb6, retrieved August 29, 2016

[52] *Fact Sheet 35: Social Networking Privacy: How to be Safe, Secure and Social*, February 2016, <https://www.privacyrights.org/social-networking-privacy-how-be-safe-secure-and-social>, retrieved August 30, 2016

[53] *FACT SHEET: Cybersecurity National Action Plan*, February 9, 2016, <https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>, retrieved August 6, 2016

[54] *FBI Suspects Russia Hacked DNC; U.S. Officials Say It Was to Elect Donald Trump*, Shane Harris, Nancy Youssef, July 25, 2016

[55] *Federal Government Hit By Major Data Breach*, June 4, 2015, <http://www.cbsnews.com/news/officials-administration-hit-by-massive-data-breach/>, retrieved August 29, 2016

[56] Federal Trade Commission, August 27, 2014, *Can you spot a government imposter?*, Amy Hebert, <https://www.consumer.ftc.gov/blog/whos-calling-not-government>, retrieved August 18, 2016

[57] Federal Trade Commission, IdentityTheft.gov, <https://identitytheft.gov/>, retrieved August 6, 2016

[58] Federal Trade Commission, March 10, 2009, *FTC Releases Spoof Videos with a Serious Message: AnnualCreditReport.com is the Only Authorized Source for Free Annual Credit Reports*, <https://www.ftc.gov/news-events/press-releases/2009/03/ftc-releases-spoof-videos-serious-message-annualcreditreportcom>, retrieved August 18, 2016

[59] Federal Trade Commission, February 9, 2015, *Government Agencies Enable HTTP Strict Transport Security for Public Websites*, Ashkan Soltani, <https://www.ftc.gov/news-events/blogs/techftc/2015/02/government-agencies-enable-http-strict-transport-security-public>, retrieved August 18, 2016

[60] Federal Trade Commission, April 2014, *Government Imposter Scams*, <https://www.consumer.ftc.gov/articles/0048-government-imposter-scams>, retrieved August 18, 2016

[61] I. Fette, N. Sadeh and A. Tomasic, *Learning to Detect Phishing Emails*, WWW 2007, May 8-12, 2007, ACM 978-1-59593-654-7/07/0005

[62] D. Florencio and C. Herley, *Evaluating a Trial Deployment of Password Re-Use for Phishing Prevention*, APWG eCrime Researcher Summit, October 4-5, 2007

[63] J. T. Ford, S. Cellan, B.F. Skinner, G. Bergmann, F.A. Breach, A. Pribram, W. Kar, *Current Trends in Psychology and the Behavioral Sciences*, University of Pittsburgh Press, 1st Ed., 1954, ASIN: B001B000I6

- [64] S. Fox, *Situated Learning Theory versus Traditional Cognitive Learning Theory: Why Management Education Should Not Ignore Management Learning*, Plenum Publishing Corporation, 1997, DOI: 10.1007/BF02557922
- [65] J. Franklin, V. Paxson, A. Perrig, and S. Savage, *An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants*, CCS'07 October 29-November 2, 2007, ACM 978-1-59593-703-2/07/0010
- [66] R. Gagne, *The Conditions of Learning*, Holt, Rinehart and Winston, 1965, ASIN: B0000B3X5E
- [67] S. Garera, N. Provos, M. Chew and A. D. Rubin, *A Framework for Detection and Measurement of Phishing Attacks*, WORM '07, November 2, 2007, ACM 978-1-59593-886-2/07/0011
- [68] M. Gaydos, *Seriously Considering Design in Educational Games*, 2015, Educational Researcher, Vol. 44, No. 9, pp 478 – 483, DOI: 10.3102/0013189X15621307
- [69] I. Granic, A. Lobel, and R. C. M. Engels, *The Benefits of Playing Video Games*, American Psychological Association, January 2014, Vol. 69, No. 1, pp 66 – 78, DOI: 10.1037/a0034857
- [70] P. Guffin, *Data Security breach Notification Requirements in the United States: WHAT YOU NEED TO KNOW*, InFOCUS Magazine December 2011, Quarterly Journal of PRISM International, <http://www.prismintl.org>, retrieved August 6, 2016
- [71] *Hacker Demonstrates How Voting Machines Can Be Compromised*, August 10, 2016, <http://www.cbsnews.com/news/rigged-presidential-elections-hackers-demonstrate-voting-threat-old-machines/>, retrieved August 31, 2016
- [72] R. Hasan and W. Yurcik, *A Statistical Analysis of Disclosed Storage Security Breaches*, StorageSS '06, October 30, 2006, ACM 1-59593-552-5/06/0010
- [73] K. Higgins, *Price Tag Rises for Stolen Identities Sold in the Underground*, December 15, 2014, <http://www.darkreading.com/attacks-breaches/price-tag-rises-for-stolen-identities-sold-in-the-underground/>, retrieved August 8, 2016
- [74] J. Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, New York Times, July 9, 2015, <http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html>, retrieved August 6, 2016
- [75] M. A. Honey and M. Hilton, Editors, *Learning Science Through Computer Games and Simulation, Chapter 3: Simulation and Games in the Classroom*, pp 57 - 62, *Chapter 7: Research Agenda for Simulation and Games*, pp 119 – 128, National Academy of Science, ISB 978-0-309-38664-7, DOI: 10.17226/13078

[76] *How People Learn: Brain, Experience, and School: Expanded Edition, Chapter 1: Learning from Speculation to Science*, National Academy of Science, pp. 3 – 27, ISB 978-0-309-07036-2, DOI: 10.17226/9853

[77] *Identity Protection: Prevention, Detection and Victim Assistance*, IRS, <https://www.irs.gov/individuals/identity-protection>, retrieved August 28, 2016

[78] *Identity Theft*, National Conference of State Legislatures, <http://www.ncsl.org/research/financial-services-and-commerce/identity-theft-state-statutes.aspx>, retrieved August 28, 2016

[79] *Identity Theft: Prevalence and Cost Appear to be Growing*, United States General Accounting Office, <http://www.gao.gov/assets/240/233900.pdf>, Retrieved July, 14, 2016

[80] Identity Theft Resource Center, June 24, 2013, <http://www.idtheftcenter.org/Identity-Theft/how-much-is-your-identity-worth-on-the-black-market.html>, retrieved August 8, 2016

[81] A. Iliya, A. Jabbar, and P. Felicia, *Gameplay Engagement and Learning Game-Based Learning: A Systematic Review*, Review of Educational Research, December 2015, Vol. 85, No. 4, pp 740 – 779, DOI: 10.3102/0034654315577210

[82] Internet Safety 101, <http://www.internetsafety101.org/>, retrieved August 6, 2016

[83] *ITRC Identity Theft Resource Center*, February 20, 2015, <http://www.idtheftcenter.org/Legislation/identity-theft-laws-around-the-country.html>, retrieved August 28, 2016

[84] T. N. Jagatic, N. A. Johnson, M. Jakobsson and F. Menezes, *Social Phishing*, Communications of the ACM, October 2007, Vol. 50, No. 10

[85] M. Jakobsson and J. Ratkiewicz, *Designing Ethical Phishing Experiments: A study of (ROT13) rOnl query features*, WWW 2006, May 23-26, 2006, ACM 1-59593-323-9/06/0005

[86] E. K. Jator, PhD, MLS(ASCP), K. Hughley, MLS(ASCP), *ABO/Rh Testing, Antibody Screening, and Biometric Technology as Tools to Combat Insurance Fraud: An Example and Discussion*, Laboratory Medicine, Winter 2014; 45(1): e3-7

[87] D. Jones, *Protecting Biometric Information in Arkansas*, Arkansas Law Review, 2016, Vol. 69 Issue 1, pp 117-142

[88] A. Jøsang, J. Fabre, B. Hay, J. Dalziel, S. Pope, *Trust Requirements in Identity Management*, Australian Information Security Workshop, 2005 (AISW 2005), Newcastle, Australia Conferences in Research and Practice in Information Technology, Vol. 44. Paul Montague and Rei Safavi-Naini, Eds., Australian Computer Society, Inc., 2005.

- [89] T. Judson MPH, M. Haas MBA, T Lagu MD MPH, *Medical Identity Theft: Prevention and Reconciliation Initiatives at Massachusetts General Hospital*, Joint Commission Journal on Quality & Patient Safety, July 2014, ; 40(7): pp 291 - 295
- [90] Y. B. Kafai, M. Resnick, Ed., *Constructionism in Practice: Designing, Thinking, and Learning in a Digital World*, Routledge; 1st Ed., April 3, 1996, ISBN-10: 0805819851, ISBN-13: 978-0805819854
- [91] Y. J. Kim, V. J. Shute, *The Interplay of Game Elements with Psychometric Qualities, Learning, and Enjoyment in Game-based Assessment*, Computers and Education, Vol. 87, 2015, pp 340–356, 0360-1315/2013, Elsevier, Ltd.
- [92] D. Kirk, *Identifying Identity Theft*, The Journal of Criminal Law, 2014, DOI: 10.1177/0022018314557418, Vol. 78(6) pp 448 – 450
- [93] R. Kling, ed., *Computerization and Controversy, 2nd Edition*, Academic Press, 1996
- [94] D. Kolb, *Experiential Learning: Experiences as the Source of Learning and Development*, FT Press, October 1, 1984, ASIN: B008UZ0U52
- [95] K. Kuutti, *Information Systems, Cooperative Work and Active Subjects: The Activity-Theoretical Perspective*, University of Oulu, 1994, ISBN-10: 9514239482, ISBN-13: 978-9514239489
- [96] B. Latour, *Science in Action: How to Follow Scientists and Engineers Through Society*, Harvard University Press, October 15, 1988, ISBN-10: 0674792912, ISBN-13: 978-0674792913
- [97] J. Lave, E. Wenger, *Situated Learning: Legitimate Peripheral Participation (Learning in Doing: Social, Cognitive and Computational Perspectives)*, Cambridge University Press, 1st Ed, September 27, 1991, ISBN-10: 0521423740, ISBN-13: 978-0521423748
- [98] L-C Lee and K-C Hao, *Designing and Evaluating Digital Game-Based Learning with the ARCS Motivation Model, Humor, and Animation*, International Journal of Technology and Human Interaction. April 2015, Vol. 11 Issue 2, pp 80 – 95
- [99] Y-H Lee, N. Dunbar, K. Kornelson, S. Wilson, R. Ralston, and M. Savic, S. Stewart, E. Lennox, W. Thompson, J. Elizondo *Digital Game based Learning for Undergraduate Calculus Education: Immersion, Calculation, and Conceptual Understanding*, International Journal of Gaming and Computer-Mediated Simulations. Jan 2016, Vol. 8 Issue 1, pp 1 – 16
- [100] A. N. Leont'ev, *Activity, Consciousness and Personality*, Prentice Hall, February 1979, ISBN-10: 0130035335, ISBN-13: 978-0130035332
- [101] *Mandatory National IDs and Biometric Databases*, <https://www.eff.org/issues/national-ids>, retrieved August 31, 2016

- [102] N. Martin, J. Rice, *Spearing High Net Wealth Individuals: The Case of Online Fraud and Mature Age Internet Users*, *International Journal of Information Security and Privacy* Volume: 7 Issue 1 (2013) ISSN: 1930-1650 Online ISSN: 1930-1669, retrieved August 1, 2016
- [103] R. C. Mathews, *International Identity Theft: How the Internet Revolutionized Identity Theft and the Approaches the World's Nations are Taking to Combat It*, *Florida Journal of International Law*, ISSN: 1556-2670, August 2013, Vol. 25 Issue 2, pp 311 - 329
- [104] A. Mathrani, S. Christian and A. Ponder-Sutton, *PlayIT: Game Based Learning Approach for Teaching Programming Concepts*, *Educational Technology & Society, Journal of Educational Technology & Society*, April 2016, Vol. 19 Issue 2, pp 5 – 17, ISSN 1436-4522 (online) and 1176-3647 (print).
- [105] R. McMahon, M. S. Bressler, and L. Bressler, *New global cybercrime calls for high tech cyber-cops*, *Journal of Legal, Ethical and Regulatory Issues*, Jan 2016, Vol. 19 Issue 1, pp 26 - 38
- [106] R. McMillan, *17 Arrested in Canadian Hacking Bust*, *PC World Communications, Inc.*, Thursday, February 21, 2008, <http://news.yahoo.com/s/pcworld/142711&printer=1>
- [107] Medicare.gov, *Help fight Medicare fraud*, <https://www.medicare.gov/forms-help-and-resources/report-fraud-and-abuse/fraud-and-abuse.html>, retrieved August 18, 2016
- [108] R. T. Mercuri, *Scoping Identity Theft*, *Communications of the ACM*, May 2006, Vol. 49, No. 5
- [109] K. Mitnick and W. Simon, *The Art of Deception*, Wiley Publishing, Inc., 2002
- [110] A. C. Moise, *Identity Theft Committed Through the Internet*, *Juridical Current*, 2015, Vol. 18 Issue 2, pp 118 - 125
- [111] T. Moore and R. Clayton, *Examining the Impact of Website Take-down on Phishing*, APWG eCrime Researchers Summit, October 4-5, 2007, Pittsburgh, PA
- [112] H. Morton, *Identity Theft Strikes Young*, *State Legislatures*, June 2014, Vol. 40 Issue 6, pp 14 – 18
- [113] *Millions of US Government Workers Hit By Data Breach*, June 5, 2015, <http://www.bbc.com/news/world-us-canada-33017310>, retrieved August 29, 2016
- [114] R. K. Myers, *“Epidemic” of Financial Fraud Techniques Targets the Elderly*, *Family and Intimate Partner Quarterly*, Fall 2015, Vol. 8 Issue 2, pp 189 -196, ISSN 1941-7462

- [115] T. Nagunwa, *Behind Identity Theft and Fraud in Cyberspace: The Current Landscape of Phishing Vectors*, International Journal of Cyber-Security and Digital Forensics. 3.1 (Jan. 2014): p72.
- [116] E. Nakashima, *Russian Government Hackers Penetrated DNC, Stole Opposition Research on Trump*, June 14, 2016 https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html, retrieved June 16, 2016
- [117] G. R. Newman, *Policy thoughts on “Bounded rationality of identity thieves”*, Criminology & Public Policy, May2009, Vol. 8 Issue 2, pp 271 - 278
- [118] R. C. Newman, CISSP, *Cybercrime, Identity Theft, and Fraud: Practicing Safe Internet – Network Security Threats and Vulnerabilities*, InfoSecCD Conference '06, September 22-23, 2006, ACM 1-59593-437-5/00/0006
- [119] D. Nicol, V. Mallapura, *Modeling and Analysis of Stepping Stone Attacks*, 2014 Winter Simulation Conference, 978-1-4799-7486-3/14/, 2014 IEEE <http://publish.illinois.edu/science-of-security-lablet/files/2014/06/Modeling-and-Analyis-of-Stepping-Stone-Attacks.pdf>
- [120] NCJRS, National Criminal Justice Reference Service, https://www.ncjrs.gov/spotlight/identity_theft/legislation.html, retrieved August 28, 2016
- [121] A. Ng, P. Watters and S. Chen, *A Consolidated Process Model for Identity Management*, Information Resources Management Journal. July-Sept, 2012, Vol. 25 Issue 3, p1, 29 p., DOI: <http://dx.doi.org/10.4018/irmj.2012070101>
- [122] T. O' Donoghue and Matthew Rabin, *The Economics of Immediate Gratification*, August 10, 1997
- [123] *Officials: Hackers Breach Election Systems in Illinois, Arizona*, August 30, 2016, <http://www.cnn.com/2016/08/29/politics/hackers-breach-illinois-arizona-election-systems/index.html>, retrieved August 31, 2016
- [124] S. Orihara, Y. Tsuruoka, K. Takahashi, *Trusted-Link: Web-Link Enhancement for Integrity and Trustworthiness*, DIM'06, November 3, 2006, Alexandria, Virginia, ACM 1-59593-547-9/06/0011
- [125] A. Pellegrini, *The Future of Play: A Multidisciplinary Inquiry into the Contributions of Brian Sutton-Smith*, State University of New York Press, August 10, 1995, ISBN-10: 0791426424, ISBN-13: 978-0791426425

- [126] A. Pellegrini, Ed., P.K. Smith, Ed., *The Nature of Play: Great Apes and Humans*, The Guilford Press; 1st Ed., December 6, 2004, ISBN-10: 1593851170, ISBN-13: 978-1593851170
- [127] *Phishing*, <https://www.consumer.ftc.gov/articles/0003-phishing>, retrieved August 9, 2016
- [128] *Phone Scams*, August 6, 2016, <https://www.consumer.ftc.gov/articles/0076-phone-scams>, retrieved August 6, 2016
- [129] J. Piaget, *Studies in Cognitive Development: Essays in Honor of Jean Piaget*, Oxford University, 1st Ed., 1969, ISBN-10: 0196318181, ISBN-13: 978-0196318189
- [130] N. L. Piquero, M. A. Cohen, and A. R. Piquero, *How Much is the Public Willing to Pay to be Protected from Identity Theft?*, *Justice Quarterly*, June 2011, Vol. 28 Issue 3, pp 437 - 459
- [131] Po-Ching Lin and Pei-Ying Lin, *Unintentional and involuntary personal information leakage on Facebook from user interactions*, *KSII Transactions on Internet and Information Systems*, July 2016, Vol. 10 Issue 7, pp 3301 - 3019
- [132] J. E. Potter, Postmaster General and CEO United States Postal Service, letter to postal customers warning of *identity theft* from February 2008
- [133] R.A. Powell, D.G. Symbaluk, P.L. Honey, *Introduction to Learning and Behavior*, Cengage Learning, ASIN: B01JXOMGBE
- [134] M. Presky, *Digital Game-Based Learning, Chapter 5: Fun, Play and Games: What Makes Games Engaging*, McGraw-Hill, 2001, pp 05-01 - 05-31
- [135] PrivacyGuard, Frank Abagnale, <https://www.privacyguard.com/frank-abagnale.html>, retrieved August 29, 2016
- [136] T. Raffetseder, E. Kirda, and C. Kruegel, *Building Anti-Phishing Browser Plug-Ins: An Experiment Report*, International Workshop on Software Engineering for Secure Systems (SESS '07), IEEE 0-7695-2952-6/07
- [137] A. Rappenport, *New Documents Released From Hack of Democratic Party*, September 13, 2016, <http://www.nytimes.com/2016/09/14/us/politics/dnc-hack.html>, retrieved September 16, 2016
- [138] L.P. Reiber, *Seriously Considering Play: Designing Interactive Learning Environments Based on the Blending of Microworlds, Simulations and Games*, 1996, *ETR&D*, Vol. 44, No. 2, pp 43 – 58, ISSN 1042-1629

- [139] C. M. Reigeluth, *Instructional Design Theories and Models: An Overview of Their Current Status*, Routledge, November 1, 1983, ISBN-10: 0898592755, ISBN-13: 978-0898592757
- [140] M. Riley, B. Elgin, D. Lawrence, C. Matlack, *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, Bloomberg News, March 17, 2015, <http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data>, retrieved August 6, 2016
- [141] W. Roberds and S. L. Schreft, *Data security, privacy, and identity theft: The economics behind the policy debates*, Economic Perspectives, Federal Reserve Bank of Chicago, Spring 2009, Vol. 33 Issue 1, pp 22 - 31
- [142] J. T. Rubens, *So Many Privacy Rules! The Developing Standard of Care for Data Security and Identity Theft Protection*, Business Law Today, 7/1/2009, Vol. 18, Issue 6, pp 54 - 58
- [143] D. Sanger, E. Schmitt, *Spy Agency Consensus Grows That Russia Hacked D.N.C.*, July 26, 2016, http://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html?_r=0, retrieved July 30, 2016
- [144] S. Schmidt, PhD and M. McCoy, *Who Is You? The Coming Epidemic of Identity Theft*, The Consortium, 2005
- [145] D. Shilling, *Financial Elder Abuse*, Family & Intimate Partner Violence Quarterly, Winter 2014, Vol. 6 Issue 3, pp 57 - 73, retrieved August 1, 2016
- [146] J. Showronski, *What Your Information is Worth on the Black Market*, <http://www.bankrate.com/finance/credit/what-your-identity-is-worth-on-black-market.aspx>, retrieved August 8, 2016
- [147] V. J. Shute and F. Ke, Assessment in Game-Based Learning: Foundations, Innovations, and Perspectives, *Chapter 4 Games, Learning, and Assessment*, 2012 Springer Science & Business Media Dordrecht, pp 43 - 58, DOI: 10.1007/978-1-4614-3546-4_4
- [148] A. D. Smith and A. R. Lias, *Identity theft and e-fraud as critical CRM concerns*, International Journal of Enterprise Information Systems. April-June, 2005, Vol. 1 Issue 2, pp 17- 37
- [149] *6 More Stores Attacked By Same Hack As Target: Firm*, Jim Finkle, January 25, 2014, http://www.huffingtonpost.com/2014/01/17/six-other-stores-are-bein_n_4618414.html, retrieved August 27, 2016
- [150] *Social Media Plagued by Privacy Problems, Researchers Say*, May 21, 2013, <http://phys.org/news/2013-05-social-media-plagued-privacy-problems.html>, retrieved August 30, 2016

- [151] *Social Networking Privacy*, <https://epic.org/privacy/socialnet/>, retrieved August 30, 2016
- [152] *Social Networking Sites: Security and Privacy Issues*, Thomas F. Duffy, September 2013, <https://msisac.cisecurity.org/newsletters/2013-09.cfm>, retrieved August 30, 2016
- [153] *Spear Phishing Angling to Steal Your Financial Info*, April 1, 2009, https://archives.fbi.gov/archives/news/stories/2009/april/spearphishing_040109, retrieved Aug 9, 2016
- [154] S. Spiekerman, J. Grossklags and B. Berendt, *E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus actual Behavior*, EC'01 October 14-17, 2001, ACM 1-58113-387-1/01/00010
- [155] R. Spinello, *Cyberethics: Morality and Law in Cyberspace, 3rd Edition*, Jones and Bartlett Publishers, 2006
- [156] *State Department: Someone Snooped in Obama's Passport File*, March 21, 2008, <http://www.cnn.com/2008/POLITICS/03/20/obama.passport/index.html>, retrieved August 30, 2016
- [157] C-H Su and C-H Cheng, *3D Game-Based Learning System for Improving Learning Achievement in Software Engineering Curriculum*, April 2013, Turkish Online Journal of Educational Technology - TOJET, Vol. 12, No. 2, pp 1 – 12
- [158] R. Sullivan, J.L. Maniff, *Data Breach Notifications*, Economic Review, 2016 1st Quarter, Vol. 101 Issue 1, pp 65-85, ISSN 0161-2387
- [159] Y. Suo, *Learning Theories Knowledge Base*, Syracuse University, <https://yasuo.expressions.syr.edu/portfolio/learning-theory-knowledge-base/>
- [160] L. Sweeney, *Data Privacy Lab SOS Social Security Number Watch*, IQSS Harvard University, <http://dataprivacylab.org/projects/ssnwatch/index.html>
- [161] L. Sweeney, *Protecting Job Seekers from Identity Theft*, IEEE March/April 2006, 1089-7801/06
- [162] *Target: 40 Million Credit Card Compromised*, December 19, 2013, <http://money.cnn.com/2013/12/18/news/companies/target-credit-card/index.html>, retrieved August 27, 2016
- [163] *Target Missed Signs of a Data Breach*, Elizabeth Harris and Nicole Perlroth, March 13, 2014, http://www.nytimes.com/2014/03/14/business/target-missed-signs-of-a-data-breach.html?_r=0, retrieved August 27, 2016

[164] *The Challenge of Health Care Fraud*, National Health Care Anti-Fraud Association, <https://www.nhcaa.org/resources/health-care-anti-fraud-resources/the-challenge-of-health-care-fraud.aspx>, retrieved August 28, 2016

[165] C. W. Thompson and D. R. Thompson, *Identity Management*, IEEE 2007, 1089-7801

[166] TransUnion, <http://www.transunion.com/>, retrieved August 29, 2016

[167] United States General Accountability Office, April 13, 2016, *2016 Annual Report: Additional Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits*, <http://www.gao.gov/assets/680/676473.pdf>, retrieved August 18, 2016

[168] United States General Accountability Office, August 20, 2014, *Identity Theft Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud*, <http://www.gao.gov/assets/670/665368.pdf>, retrieved August 18, 2016

[169] United States General Accountability Office, May 24, 2016, *Identity Theft and Tax Fraud IRS Needs to Update Its Risk Assessment for the Taxpayer Protection Program*, <http://www.gao.gov/assets/680/677406.pdf>, retrieved August 18, 2016

[170] United States General Accountability Office, June 23, 2016, *Identity Theft Tax Refund Fraud*, <http://www.gao.gov/multimedia/podcasts/677925>, retrieved August 18, 2016

[171] United States General Accountability Office, November 29, 2012, *Identity Theft Total Extent of Refund Fraud Using Stolen Identities is Unknown*, <http://www.gao.gov/assets/660/650365.pdf>, retrieved August 18, 2016

[172] United States General Accountability Office, April 12, 2016, *Information Security IRS Needs to Further Improve Controls over Taxpayer Data and Continue to Combat Identity Theft Refund Fraud*, <http://www.gao.gov/assets/680/676493.pdf>, retrieved August 18, 2016

[173] United States General Accountability Office, April 19, 2016, *Tax Filing: IRS Needs a Comprehensive Customer Service Strategy and Needs to Better Combat Identity Theft Refund Fraud and Protect Taxpayer Data*, <http://www.gao.gov/assets/680/676675.pdf>, retrieved August 18, 2016

[174] United States Sentencing Commission, *An Overview of Loss in USSG §2B1.1*, April 2009, http://www.ussc.gov/sites/default/files/pdf/training/online-learning-center/supporting-materials/Loss_Overview_2009_April.pdf, retrieved August 15, 2016

[175] United States Sentencing Commission, *Identity Theft and Assumption Deterrence Act of 1998*, <http://www.ussc.gov/sites/default/files/pdf/research-and-publications/working-group-reports/intellectual-property-and-tech/19991215-identity-theft/AppendA.pdf>, retrieved August 15, 2016

- [176] U.S. Sentencing Commission, Policy Papers December 15, 1999, *Identity Theft: Final Report*, <http://www.ussc.gov/research/research-and-publications/united-states-sentencing-commission-economic-crimes-policy-team>, retrieved August 15, 2016
- [177] United States Sentencing Commission, *United States Code*, <https://www.gpo.gov/fdsys/browse/collectionUSCode.action?collectionCode=USCODE>, retrieved August 15, 2016
- [178] W. Veeneman, I. Mayer, *Games in a World of Infrastructure: Simulation-Games for Research, Learning and Intervention*, Eburon B V, 2004, ASIN: B01MFAERA9
- [179] *Voting Machines Can Be Easily Compromised, Symantec Demonstrates*, August 13, 2016, <https://it.slashdot.org/story/16/08/13/1553237/voting-machines-can-be-easily-compromised-symantec-demonstrates>, retrieved August 31, 2016
- [180] L.S. Vygotsky, *Mind in Society: The Development of Higher Psychological Processes*, 14th Ed., ASIN: B006OR5INC
- [181] L.S. Vygotsky, *Thought and Language*, MIT Press, 1962, ASIN: B00BWJ5R88
- [182] A. Walters & R.H. Bandura, *Social Learning and Personality Development*, Holt, Rinehart and Winston, 1965, ASIN: B013KQYBFU
- [183] W. Wang, Y. Yuan and N. Archer, *A Contextual Framework for Combating Identity Theft*, IEEE, 1544-7993/06
- [184] B. Weiner, *Achievement, Motivation, and Attribution Theory*, General Learning Press, 1st Ed., 1974, ISBN-10: 0382250664, ISBN-13: 978-0382250668
- [185] *Wells Fargo is Fined Record-Breaking \$190 million and Fires 5,300 Staff After 'Widespread' Customer Fraud Scheme is Uncovered*, Chris Pleasance, September 8, 2016, <http://www.dailymail.co.uk/news/article-3780625/Wells-Fargo-fined-record-breaking-190million-fires-5-300-staff-widespread-customer-fraud-scheme-uncovered.html>, retrieved September 12, 2016
- [186]J-C. Woo, *Digital Game-Based Learning Supports Student Motivation, Cognitive Success, and Performance Outcomes*, 2014, Educational Technology & Society, 17 (3), 291 – 307, ISSN 1436-4522 (online) and 1176-3647 (print), pp 291 - 307.
- [187]M. Wu, R. C. Miller, and G. Little, *Web Wallet: Preventing Phishing Attacks by Revealing User Intentions*, Symposium On Usable Privacy and Security (SOUPS) 2006, July 12-14, 2006

[188]W-H. Wu, H-C. Hsiano, P.L. Wu, C-H Lin, and S-H. Huang, *Investigating the Learning-theory Foundations of Game-based Learning: A Meta-analysis*, Journal of Computer Assisted Learning, 2012, Vol. 28, pp 265-279

[189] T.D. Yawkey, Ed., A.D. Pellegrini, Ed., *Child's Play and Applied (Child Psychology)*, Psychology Press; First Edition, 1st Ed., January 1, 1984, ISBN-10: 089859300X, ISBN-13: 978-0898593006

APPENDIX A

INSTITUTIONAL REVIEW BOARD DOCUMENTS

Institutional Review Board Letter of Approval

IOWA STATE UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Institutional Review Board
Office for Responsible Research
Vice President for Research
1138 Pearson Hall
Ames, Iowa 50011-2207
515 294-4566
FAX 515 294-4267

Date: 7/15/2014
To: Susan Helsler
2081 Scott Rd
North Branch, MI 48461
From: Office for Responsible Research
Title: Identity Theft Education: A Comparison of Game-Based and Text-Based Information Delivery Methods
IRB ID: 14-324
Approval Date: 7/10/2014
Submission Type: New
Date for Continuing Review: 7/9/2016
Review Type: Expedited
CC: Dr. Doug Jacobson
202 Nuclear Engineering

The project referenced above has received approval from the Institutional Review Board (IRB) at Iowa State University according to the dates shown above. Please refer to the IRB ID number shown above in all correspondence regarding this study.

To ensure compliance with federal regulations (45 CFR 46 & 21 CFR 56), please be sure to:

Use only the approved study materials in your research, including the recruitment materials and informed consent documents that have the IRB approval stamp.

Retain signed informed consent documents for 3 years after the close of the study, when documented consent is required.

Obtain IRB approval prior to implementing any changes to the study by submitting a Modification Form for Non-Exempt Research or Amendment for Personnel Changes form, as necessary.

Immediately inform the IRB of (1) all serious and/or unexpected adverse experiences involving risks to subjects or others; and (2) **any other unanticipated problems involving risks** to subjects or others.

Stop all research activity if IRB approval lapses, unless continuation is necessary to prevent harm to research participants. Research activity can resume once IRB approval is reestablished.

Complete a new continuing review form at least three to four weeks prior to the **date for continuing review** as noted above to provide sufficient time for the IRB to review and approve continuation of the study. We will send a courtesy reminder as this date approaches.

Please be aware that IRB approval means that you have met the requirements of federal regulations and ISU policies governing human subjects research. **Approval from other entities may also be needed.** For example, access to data from private records (e.g. student, medical, or employment records, etc.) that are protected by FERPA, HIPAA, or other confidentiality policies requires permission from the holders of those records. Similarly, for research conducted in institutions other than ISU (e.g., schools, other colleges or universities, medical facilities, companies, etc.), investigators must obtain permission from the institution(s) as required by their policies. **IRB approval in no way implies or guarantees that permission from these other entities will be granted.**

Upon completion of the project, please submit a Project Closure Form to the Office for Responsible Research, 1138 Pearson Hall, to officially close the project.

Please don't hesitate to contact us if you have questions or concerns at 515-294-4566 or IRB@iastate.edu.

Identity Theft Flyer



ISU IRB # 1	14-324
Approved Date:	6 July 2016
Expiration Date:	9 July 2018

Susan Helser

Identity Theft Research for PhD degree

Iowa State University
Department of Electrical and Computer Engineering

Doug Jacobson, PhD, Committee Chair

This is a research study. Please take your time in deciding if you would like to participate. Please feel free to ask questions at any time.

The purpose of this study is to investigate contributing factors to identity theft that include individuals' 1) misconceptions prior to the occurrence of an event, 2) lack of knowledge of the consequences that can follow an event, and 3) jargon associated with an event.

You are being invited to participate in this study because you are a college student and are 18 years of age or older. If you are not a college student or you are younger than 18 years of age you should NOT participate in this study.

Participation in the study does not affect your grade in this course.

If you agree to participate, you will be asked to 1) supply demographic information, 2) complete short surveys prior to and following exposure to educational materials and 3) comment on the experience.


Your individual responses will be kept in strict confidence. Your personal information will not be associated with your response. The researchers will be the only individuals who have access to the data. If the results are published, your identity will remain confidential.

There are no foreseeable risks from participating in this study. Your participation in this study is completely voluntary. If you do not feel comfortable completing the study, you are free to discontinue at any time. There is no penalty or loss to you for not completing the study or if you begin the study but wish to withdraw and discontinue. However, we would appreciate if you would complete the entire study. By participating, you give the researchers your consent. The study should take less than 30 minutes of your time.

You are encouraged to ask questions at any time during this study. For further information about the study contact Susan Helser, (810) 265-1376, shelser@iastate.edu; Dr. Doug Jacobson, (515) 294-8307, dougj@iastate.edu. If you have any questions about the rights of research subjects or research-related inquiry, please contact the IRB Administrator, (515) 294-4566, IRB@iastate.edu, or Director, (515) 294-3115, Office of Research Assurances, 1138 Pearson Hall, Iowa State University, Ames, Iowa 50011.

Your efforts in participating in this research project are deeply appreciated.

Contact: Susan Helser, shelser@iastate.edu



Recruitment Email

ISU IRB # 1	14-324
Approved Date:	6 July 2016
Expiration Date:	9 July 2018

SUBJECT: Invitation to Research Study on Identity Theft

BODY:

Dear Student,

I invite you to participate in a research study in which you would: 1) supply demographic information, 2) complete short surveys prior to and following exposure to educational materials, and 3) comment on the experience. This study is conducted on a computer and requires about 30 minutes to complete.

The purpose of this study is to investigate contributing factors to identity theft that include individuals' 1) misconceptions prior to the occurrence of an event, 2) lack of knowledge of the consequences that can follow an event, and 3) jargon associated with an event.

You may participate if you are 18 years of age or older and are a college student. You should NOT participate if you are younger than 18 or are not a college student.

Participation in this study is completely optional and will not affect your grade in the course.

Your efforts in participating in this research project are deeply appreciated.

If you would like to participate in this study, please write to me to indicate your interest. My name and email address are Susan Helsler and (shelsler@iastate.edu), respectively. I will forward a copy of the informed consent to you for your consideration. After receiving the informed consent, please read the document and decide whether you want to proceed with the research. If you agree to participate, then Susan Helsler will tell you the computer lab where the research will occur.

Thank you,
Susan Helsler
Principal Investigator

Invitation Script

ISU IRB # 1	14-324
Approved Date:	6 July 2016
Expiration Date:	9 July 2018

SUBJECT: Invitation to Research Study on Identity Theft

BODY:

Dear Student,

I invite you to participate in a research study in which you would: 1) supply demographic information, 2) complete short surveys prior to and following exposure to educational materials, and 3) comment on the experience. This study is conducted on a computer and requires about 30 minutes to complete.

The purpose of this study is to investigate contributing factors to identity theft that include individuals' 1) misconceptions prior to the occurrence of an event, 2) lack of knowledge of the consequences that can follow an event, and 3) jargon associated with an event.

You may participate if you are 18 years of age or older and are a college student. You should NOT participate if you are younger than 18 or are not a college student.

Participation in this study is completely optional and will not affect your grade in the course.

Your efforts in participating in this research project are deeply appreciated.

If you would like to participate in this study, please read and consider the informed consent document. If you agree to participate, then I will tell you the computer lab where the research will occur.

Thank you,
Susan Heiser
Principal Investigator

This study is conducted under the direction of Dr. Doug Jacobson, Committee Chair, in Department of Electrical and Computer Engineering in the College of Engineering at Iowa State University

Informed Consent

ISU IRB # 1	14-324
ISU IRB # 1	14-324
Approved Date:	6 July 2016
Expiration Date:	9 July 2018

software's experience survey asks you for feedback about your experience learning about identity theft.

Your participation should take less than 30 minutes. The surveys should take about 10 minutes and the educational module should take about 10 minutes.

What are the possible risks or discomforts and benefits of my participation?

Risks or Discomforts—The possible risks related to your participation in this research are only those associated with everyday computer usage.

Benefits—You may not receive any direct benefit from taking part in this study. We hope that this research will benefit society but, you will have the opportunity to learn about identity theft and its consequences. If you are a student, you may gain an educational benefit of better understanding the nature of the research or concepts described in your classes.

How will the information I provide be used?

The information you provide will be used for the following purposes: The principal investigator and faculty supervisor will be the only people who have direct access to the data. The information that is gathered will be used to assess the two different educational methods.

What measures will be taken to ensure the confidentiality of the data or to protect my privacy?

Information that you provide that relates to your identity such as gender or age range will remain confidential. Data will be collected on a flash drive during the study. It will be transferred from the flash drive to a computer for analysis where it will be encrypted and stored. After data is transferred to the computer from the flash drive it will be removed from the flash drive. The computer that will be used to do the analysis is stored securely, password protected and has anti-virus software installed. Records identifying participants will be kept confidential to the extent allowed by applicable laws and regulations. Records will not be made publicly available. However, federal government regulatory agencies, auditing departments of Iowa State University, and the ISU Institutional Review Board (a committee that reviews and approves research studies with human subjects) may inspect and/or copy study records for quality assurance and analysis. These records may contain private information.

To ensure confidentiality to the extent permitted by law, the following measures will be taken: In the recruitment period information about the research will be presented and discussed. Students will not be singled out during this process and are free to not take part at any time. Prior to the start of the study, the Principal Investigator will insert a flash drive that contains the software application into each computer in the lab where the research will occur. After a participant completes the project, the Principal Investigator will collect the flash drives and then transfer data to a computer for analysis. The Principal Investigator and Supervising Faculty are the only people who will view the data.

Will I incur any costs from participating or will I be compensated?

You will not have any costs from participating in this study. You will not be compensated for participating in this study.

What are my rights as a human research participant?

Participating in this study is completely voluntary. You may choose not to take part in the study or to stop participating at any time, for any reason, without penalty or negative consequences.

ISU IRB # 1	14-324
Approved Date:	6 July 2016
Expiration Date:	9 July 2018

Regardless of the number of your classmates who take part in this study, you are not required to participate in the research. Participation is not a component of your course grade and will not affect your outcome in the class in any way.

If you have any questions *about the rights of research subjects or research-related injury*, please contact the IRB Administrator, (515) 294-4566, IRB@iastate.edu, or Director, (515) 294-3115, Office for Responsible Research, 1138 Pearson Hall, Iowa State University, Ames, Iowa 50011.

What if I am injured as a result of participating in this study?

There is no foreseeable risk of injury if you choose to participate in the study.

Whom can I call if I have questions about the study?

You are encouraged to ask questions at any time during this study. For further information, please contact Susan Helsler (PI), shelsler@iastate.edu, 810-265-1376; Doug Jacobson, PhD (Major Professor), dougi@iastate.edu, 515-294-8307.

Consent and Authorization Provisions

Your signature indicates that you voluntarily agree to participate in this study, that the study has been explained to you, that you have been given the time to read the document and that your questions have been satisfactorily answered. You will receive a copy of the written informed consent prior to your participation in the study.

Participant's Name (printed)

Participant's Signature Date

APPENDIX B

FIGHT IDENTITY THEFT (FIT) INTRODUCTION PANEL

Dear Participants:

This study is being conducted by Susan Helser (Ph.D. student) and Drs. Doug Jacobson (Committee Chair), Thomas Daniels, Jennifer Davidson, Stephen Gilbert, Steffen Schmidt in Department of Electrical and Computer Engineering in the College of Engineering at Iowa State University.

This is a research study. Please take your time in deciding if you would like to participate. Please feel free to ask questions at any time.

The purpose of this study is to investigate contributing factors to identity theft that include individuals' 1) misconceptions prior to the occurrence of an event, 2) lack of knowledge of the consequences that can follow an event, and 3) jargon associated with an event.

You are being invited to participate in this study because you are 18 years of age or older. You should NOT participate if you are younger than 18.

If you agree to participate, you will be asked to 1) supply demographic information, 2) complete a short surveys prior to and following exposure to educational materials, and 3) comment on the experience.

Your individual responses will be kept in strict confidence. Your personal information will not be associated with your response. The researchers will be the only individuals who have access to the data. If the results are published, your identity will remain confidential.

There are no foreseeable risks from participating in this study. Your participation in this study is completely voluntary. If you do not feel comfortable completing the study, you are free to discontinue at any time. There is no penalty or loss to you for not completing the study or if you begin the study but wish to withdraw and discontinue. However, we would appreciate if you would complete the entire study. By participating, you give the researchers your consent. The study will take about 20 minutes of your time.

Your efforts in participating in this research project are deeply appreciated.

Do you agree to participate in this survey? This question is required.
Click the Start button to begin.

APPENDIX C

DEMOGRAPHIC INFORMATION

Sex text and possible responses follow.

I am

Male, Female

Age text and possible responses follow.

My age group is

less than 18; 18 to 22; 23 to 30; 31 to 45; 46 and above

Education text and possible responses follow.

My highest level of education is

some high school; high school graduate; one year college; two years college; more than two years college

Major text follows. This is an open response area.

My major study area is

(open response)

Tech savvy text and possible responses follows.

My tech savvy level is

low; low to medium; medium; medium to high; high

APPENDIX D

SURVEY 1 AND SURVEY 2 QUESTIONS

Questions are grouped in three areas that consider the participant's *lack of knowledge following an event* (Questions 1, 2, 7), *misconceptions prior to the occurrence of an event* (Questions 3, 6, 8), and *jargon* (Questions 4, 5, 9).

Question 1: Identity theft can lead to credit problems.

Question 2: Medical insurance can be denied, because of identity theft.

Question 3: It is smart to buy from the cheapest online vendor.

Question 4: Phishing can occur at work.

Question 5: Social engineering is a form of social media.

Question 6: It's okay to stay logged on to a computer when you leave it for a few minutes.

Question 7: Purchases that you don't make don't impact your credit.

Question 8: Social media sites are good places to share your information.

Question 9: Cell apps are reliable.

APPENDIX E

FIT INFORMATION

Finance

Magnetic Ink Character Recognition also known as MICR, is encoding utility used for character recognition to process checks and other documents in the financial services industry. The data is listed in clear view on the bottom of the item in the MICR Line and includes a document type, bank code (unique bank identifier; in US, routing transit number), bank account number (unique customer number), check number, value and a control sequence. The MICR font used in the US is called MICR E-13B. It includes ten digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, and four other special characters used to bracket the unique identifiers in the MICR line.

Routing Transit Number also known as RTN, is a nine digit unique identifier used in the United States that is included on the lower portion of financial documents such as checks. In addition, in the United States the RTN is used for electronic transfers by the Federal Reserve Bank (FRB) to process Fedwire and by Automated Clearing House (ACH) to handle a variety of transactions such as direct deposit and bill payments.

One possible outcome of identity theft is that the victim is unable to qualify for credit when she or he applies for loans. The reason for this is that, unknown to the victim whose identity has been stolen, the thief has acquired substantial debt in the victim's name. It is likely that the thief has not made a payment on the debt, so the victim's credit is negatively impacted. Even if the thief has made payments, the debt associated with the victim is likely large enough to result in denial of new credit.

A possible outcome of identity theft for the victim is that, if credit is awarded, the interest rate that is available will be high. The reason for this is that the thief has acquired substantial debt in the victim's name. It is likely that the thief has not made payments which, in turn, affects the victim's credit score. Even if the thief has made payments, the debt tied to the victim is likely substantial and will impact the interest rate that is available.

Homebanking represents a convenient and useful option to traditional banking methods. It is important to have good virus protection software installed on a computer that is used for homebanking. In addition, it is necessary to receive regular virus protection updates so that the computer is protected from current threats.

Limit visual access to checks written in public places to deter check fraud. For example, if an identity thief is able to take a picture of a victim's check, it is then possible for the thief to order new checks from a source other than the bank where the account is located. The new checks work in just the same way as checks the account holder has in her or his possession, so the thief is able to make purchases.

Health

The Contract Number or Health Insurance Contract Number, is a unique number associated with an individual who holds a health insurance policy with a company such as Aetna, Blue Cross, Cigna or another carrier. The policy holder the primary account and in addition to the Contract Number is, generally, assigned the number 1. Family members have the same Contract Number, but are given other identifiers such as 2, 3, etc. For this reason, a Contract Number may have several individuals associated with it. At one time the policy holder's Social Security Number was used as the Contract Number, but this practice is no longer in use.

Script Fraud also known as Prescription Fraud is the false use of a policy holder's prescription drug benefit. Once the insured party's health insurance information is compromised, an identity thief is able to access the prescription benefit. Fraudulent scripts can be written for drugs in the policy holder's name and then sold by the identity thief. Medications may become unavailable to the policy holder, because a limit has been reached.

One possible outcome of identity theft is that the victim's health record is incorrect. Inaccurate records may reflect conditions that do not exist, surgeries that have not been performed and affect decisions that are made in subsequent patient care. Bogus data associated with the policy holder can impact options at the time of a subsequent emergency. Substantial copays, deductibles, and other charges may be assessed to the policy holder.

A possible result of identity theft is that benefits the policy holder is entitled to may be unavailable. A maximum amount for a particular condition or service such as an eye exam with new lens or physical therapy may have been used by the identity thief. If this is the case, when the policy holder attempts to access the resources associated with the benefit the claim is denied. The time that is necessary to straighten out such an issue can be significant.

Online access to medical records represents a convenient and useful option to traditional methods. Good virus protection software on the computer that is used to examine online medical records is imperative. In addition, it is necessary to receive regular virus protection updates so that the computer is protected from current threats.

Medical insurance fraud such as false billing for services and procedures to carriers accounts for hundreds of millions of dollars in loss each year. The identity thief could be an individual operating independently and infrequently or someone who works for a provider facility such as a hospital and is a member of a team that submits thousands of bogus claims. In either case, the health insurance company that has been billed pays the claim submitted in the policy holder's name.

Entertainment

A Social Network is an organization that consists of members who abide by and operate within a set of rules. As the Social Network develops, the interaction that occurs between pairs or groups of individuals impacts the members and is reflected in the behavior and

practices of the organization. Online cases include, billboards and chat rooms. Research has shown that individuals behave differently when engaged in these environments. For example, people reveal personal information that ordinarily they would not do or create elaborate personas that have no resemblance to themselves. Either case can lead to serious consequences.

Too Good To Be True Events represent a windfall for the identity thief with little recourse for the victim. Contributing factors to the swindle are the short window of time and electronic distribution. For example, immediately after the exchange of a real pair of tickets for another set, if the original tickets fall into the hands of a thief, the crook can sell them to one or more online buyers. Bogus tickets may be sent to the victim. On event day the mark learns of the misfortune.

One misconception related to credit card fraud, a form of identity theft, is that it is a victimless crime. This is clearly not the case. For example, problems include the impact on the victim's credit report; time lost by the victim spent to address issues connected to the compromised credit card; higher prices for goods and services that must be covered up by the seller due to loss through theft. The idea that someone else will fix the problem and that it will go away by itself is false, too.

Bogus Bargain Travel intended to get a victim to reveal personal information can lead to identity theft. A promotional travel package offered at a great price or free in a contest may, in fact, be the attack vector used by the identity thief to lure an unsuspecting victim into providing unique identity data such as address, age, gender, credit card or bank account numbers. These scams are easy to perpetrate over the Internet. Once information has been submitted in an online form it is gone.

One misconception regarding room rentals is that nothing of consequence can go wrong which is untrue. Stay at inns that require photo ID to prove that you are the person who made the reservation. An identity thief could make a reservation over the phone with a stolen credit card number. An ID check at the desk will prevent the thief from accessing resources available at inns.

Lost or stolen ID information is serious. An identity thief with access to real identity documents can do virtually anything the actual victim could do in her or his name. For example, some activities could include applying for credit cards, taking out a mortgage, purchasing a car or another large ticket item, and signing up for student loans. Clearing your name after fraudulent purchases are made by a thief is time consuming, costly, and can have significant long term consequences.

Work

Weak passwords represent 25% of all passwords and are a security risk. They offer little protection to the person who selects them and provide the identity thief with access to the individual's resources. Several examples of weak passwords include default passwords set by the manufacture at the factory, birthdates, addresses, hobbies, sports, and names of children or pets. Data that can be learned via online searches and other methods of discovery should be avoided as passwords. Weak passwords can be limited by choosing a combination of letters of both cases, numbers and special characters such as the underscore or ampersand.

Password Sharing eliminates unique access by an individual to resources and services. It represents a substantial security risk, since whoever supplies the correct password enjoys the privileges of the account holder. It is easy for the identity thief to exploit the weakness. A thief offers help to the victim who is having difficulty. The person provides requested login information to the thief who tucks it away for future use after the immediate issue has been addressed.

Unprotected computers which include systems without the latest release of software loaded are a security risk. They can provide identity thieves with access to confidential information. Once an authorized user's account has been compromised, employer data is available to the thief. Virus protection and other software updates from the manufacture should be installed as soon as they are released to limit vulnerabilities related. Corporate espionage is a direct consequence.

Identity thieves posing as visitors or guests from another division of the business are a security threat. Once inside the establishment the thief may be able to access internal networks reserved for employees. They should not be left unsupervised in a room with network connections. The receptionist, secretaries and others who meet the public should receive regular training about guest related procedures. Employees must follow corporate policies established to protect the business.

Resumes should not contain personal and detailed information such as a social security number, references or professional licenses. Reserve this information for the job application. Thieves harvest the data to build identities. The thief posing as a prospective employer requires references that are, in turn, sent to another company where the crook will commit crime in the victim's name.

Personal documents must be handled appropriately. Documents that are to be kept should be stored in a secure manner. Those that are to be discarded should be shredded with a cross-cut shredding machine to reduce the material to tiny pieces. Identity thieves "dumpster dive" or forage in trash piles and receptacles. They collect information and use to construct an identity then exploit resources and leave a mess for the victim to clean up.

Home

Unknown callers are a security threat. An identity thief may pose as person who has called a wrong number, a charity worker, or someone phoning to award a prize. The identity thief may call several times over a period of weeks in order to establish a relationship with the victim. During this time the thief learns confidential information. Vulnerable populations such as the elderly are easily exploited. Check on older family members and remind them not to give out private information over the telephone. If a request for medical records is received, have the senior write down the phone number and then help the senior by returning the call later.

Mailboxes exist in physical reality and cyberspace. Once compromised, both represent vulnerabilities for the same reasons. Potentially both hold identity information that thieves seek. In physical reality, confidential materials such as statements and reports arrive via mailboxes. Many of the same type of documents may be received in the online box. An additional issue related to the virtual box is that the thief can send messages that look like they have come from the victim.

Not all shredders are created equal. Disposing of personal documents by shredding them with a cross-cut shredder is necessary. These machines may cost more than other shredders, but they produce a finer, and therefore, better result. Cross-cut shredders reduce documents to bits the size of confetti. Tiny fragments of paper are more difficult to piece back together than is a pile of spaghetti cut paper that can be reassembled into the original document in a short time.

Change goes hand in hand with moving. Identity thieves are aware of transfer of ownership and exploit resources during the transition period. Because of the number of things in flux during a move, the new property owner is at risk. The identity thief can make purchases while the new owner is getting settled. In one case, thieves posed as new home owners and took possession of a car from a dealership in the community leaving the real newcomers with a huge mess to clean up.

Statistics show that family members make up a substantial percent of identity thieves. A parent may steal a spouse's or child's identity in order to get more credit. This is not uncommon after a divorce. A cousin, aunt, uncle, or sibling may steal a family member's identity. It is possible that the identity of a deceased member of the family may be stolen which is particularly difficult for parents.

Announcements of engagements, marriage, births, deaths, travel and other periods of transition should be limited to the recipients that should receive the information. Broadcast messages over email, social media or in publications that contain such information is the identity thief's bread and butter and should be avoided. Transition periods are easy for the thief to exploit and provide a window of opportunity.

Education

Prevent unwelcome eavesdroppers from gaining direct access to your student account or login information. Student loan funds transferred from the loan recipient's account to another location are the recipient's responsibility. Unlike some other forms of financial fraud in which the victim does not have to make good on the bill, the money that an identity thief electronically moves from a student's financial aid account to some other destination must be repaid. The individual who took out the loan is financially obligated to foot the cost of the stolen money. A legal action against the identity thief could result in recovery of funds in the future.

All email messages are not created equal. Bogus messages are often intended to generate a particular response from the victim. The originator of the bogus email preys on human vulnerabilities to manipulate the victim. The solicitation of funds to help those in need following a natural disaster or an offer of a too good to be true windfall are two examples. Make sure to confirm the sender's identity before deciding to enter information in an online form that cannot be recovered.

Phishing, rather than the legitimate activity of fishing, is the cyber name for hooking and catching a victim using tools such as bogus emails via the Internet. Phishing emails may arrive in your mailbox directly from an identity thief or from someone you know and trust, but whose email has been hijacked by a fraudster. In a phishing attack the thief "throws out the net" to catch as many victims as possible. "Spear phishing" is a related technique in which the perpetrator targets a select group.

Compromised ID is a term used to indicate that an identity has been stolen. The extent of the consequences of identity theft vary. For example, student login information may be abused to generate malicious or threatening email to a fellow student, member of the faculty, or to someone outside of the institution; to acquire authentic academic records for future use; or to move resources such as financial aid funds to another account.

Protect your student identification to prevent identity thieves from getting copies of your academic record. A copy of an academic transcript is required for certain jobs. The identity thief who has access to your academic record can use it as proof of a degree to gain access to an institution, take out student loans, or seek employment in your name.

Students are valuable to identity thieves, because often they initially have good credit and their incomes increase over time. Unknown purchases made by a fraudster in the name of the victim can impact the victim's life years later. An individual's credit can be ruined or damaged. If credit is available, it can be costly with high interest rates set for loans and credit cards to take into account the risk associated with lending to an individual with bad credit.

Shopping

Misplaced or otherwise out of sight credit cards can affect a credit score, since purchases go through the credit reporting process. Once a card number and authorization code are known to a thief, unauthorized use is possible. For example, if a card leaves the table at a restaurant, information can be recorded for later use. Items can be acquired using the stolen card number without the card through a web application or telephone sale. Purchases made without the owner's consent are often not the responsibility of the card holder, but marks placed on the credit report impact the owner's ability to get credit and rates that are available.

Unauthorized purchases can negatively affect the credit score of the card holder which impacts her or his ability to acquire credit in the future and available interest rates. An identity thief can run up charges on the account owner's credit card. Unpaid balances reflect the indebtedness of the card holder. The greater the debt, the less likely it may be possible to get credit and the higher the lending rate that will be available.

Online scams include the collection of information. A survey may ask a respondent to rate items. Initial questions appear harmless, but later some are slipped in that require personal information such as gender, date of birth or zip code. The sale of items below market value is another technique used to hook victims. A buyer receives goods for a great price, but in doing so must transfer information such as address and credit card to the identity thief.

Unknown charge accounts can negatively affect the credit score of the card holder whose name is associated with it. Bogus accounts can be set up in a victim's name. When card maximums are reached, even if the minimum payment is made by the identity thief, the indebtedness impacts the victim's credit score. Often purchases are for items that can be quickly turned around and sold for cash which makes it difficult to combat this crime.

A compromised checking account occurs when identifiers for an account such as the number, bank identification number and perhaps PIN become known to an identity thief. The crook orders checks with the account owner's account data then receives and uses them. Funds are removed from the owner's account to cover the checks since the bank assumes that they are real.

Providing unnecessary information to another party on the telephone, online or in person puts a person at risk of becoming a victim of identity theft. Information such as date of birth, zip code and gender uniquely identify about 87.5% of the population in the U.S.A. If a seller has no need for a piece of identity information, do not provide it. Thieves assemble data over time. Information collected years earlier can be combined with more recent material to build an identity for future use.

Communication

Care should be taken to avoid the disclosure of personal information in public via cell phones and pay phones. Identity thieves situated in any public space can record important data such as birthdates, home or work addresses, time schedules, and charge account information by simply eavesdropping. A variety of tools exist that the identity thief can use to discretely harvest material for future use or perhaps sale to a third party. Devices range from very basic to highly sophisticated recording equipment. Information revealed to the identity thief may be exploited in the future and, therefore, go unnoticed for a period of time.

Social Media represents fertile ground for identity thieves. Privacy options designed to provide security, generally, are not the default setting and must be activated by the user. This is consistent with Social Media as its purpose is to share information. Unless a user chooses to opt out and specifies exactly who may have access to information, data on the site is available to a host of individuals including possibly identity thieves.

Unprotected email accounts provide an avenue for identity thieves to exploit. This resource can be used for purely malicious purposes such as to send threatening messages to a third party or to solicit goods and services in the victim's name. Consequences can be dire for a person whose email account has been compromised. Consider the outcome from a threat sent to the President of the United States.

Social Engineering is a collection of methods and techniques used by a fraudster to build a relationship and gain the trust of a future victim. Over time an identity thief develops a line of communication with the individual who will be exploited. The idea is that familiarity will erode boundaries to produce the desired result. For example, phone calls from an alleged realtor with information about home values may be a guise from an identity thief bent on collecting personal data.

Trojans and bots are names for malicious and deliberately concealed programs with a hidden agenda that run on electronic devices. Risks include the collection of personal information returned to the botmaster, an identity thief, often far from the victim. The Trojan secretly invades a device while the bot, short for robot, spies on the system then relays data back to the botmaster.

Not all web pages on the Internet are equal. Those that are infected may contain malware programs that present a significant threat to victims who visit the sites. Malware is intended to do harm and is controlled by a third party such as an identity thief. The collection of personal information via key-logging programs to record keystrokes of a victim and then forward the information to the fraudster is one possible result. It is important to regularly update virus protection software.

Mobile Device

War Driving is when an unauthorized user, perhaps an identity thief, accesses an unprotected wireless network for personal gain. The term is derived from the practice of driving a vehicle in search of resources that are available via a private, but open network. The vulnerability could be due to a lack of knowledge on the part of the account holder of Internet settings on the device that is used to connect to the web. The unprotected network allows the war driver to use resources paid for by the victim. For example, large files may be transferred by the thief without the knowledge of the account holder with the resulting data charges billed to the victim.

The majority of current cell phone applications have few or no security features. This is due in part to the fact cell apps have been designed with convenience in mind as the prime focus. Personal information such as addresses or pictures and contact data for friends and family members is readily available to the cell owner, but also is only fingertips away for the identity thief who has walked off with a victim's phone. Keep cell phones in a secure place at all times to avoid data loss.

The majority of current cell phones and a variety of other mobile devices possess weak or no security options. Data stored on them is, therefore, at risk of being compromised by an identity thief who steals the device. Calendars, birthdates, addresses, credit card numbers, passwords, anything saved on the system represents a resource to exploit by an identity thief. The stolen device could also be used to commit fraud in its owner's name which may require countless hours to resolve.

PDA aka Personal Digital Assistant is an acronym used for a host of small hand held devices designed to store user data such as phone numbers, addresses, calendars, passwords and other pieces of information. Devices are often loaded with personal data and are targeted by identity thieves ready to help themselves. The information acquired from a PDA can be used to build bogus accounts based on actual human data which presents a real challenge for law enforcement.

Digital cameras record more than the image that the user wants to save. Unless specific options are disabled, digital cameras also record information such as GPS location data and time a related timestamp. This material may be sensitive, if it leaks information to an identity thief about the photographer's family, schedule, address, habits or other preferences. Cell phones are small specialized computers and as such are subject to computer viruses just as are larger computer systems. Trojans and other virus programs can steal or corrupt data stored on a cell phone. Substantial quantities of information that identity thieves can exploit is available on cell phones. Thieves target the devices and can access data via electronic transfer with methods similar to those used on other systems.

APPENDIX F

PARTICIPANT FEEDBACK PANEL

The *Participant Feedback Panel* contains three areas for the participant to indicate his or her perceptions regarding the study that include *My Benefit Level*, *My Enjoyment Level* and *My Comments*.

My Benefit Level responses are chosen from a list of five options that include: 1) No Opinion, 2) Not Beneficial, 3) Slightly Beneficial, 4) Moderately Beneficial, and 5) Very Beneficial.

My Enjoyment Level responses are chosen from a list of five options that include: 1) No Opinion, 2) Not Enjoyable, 3) Slightly Enjoyable, 4) Moderately Enjoyable, and 5) Very Enjoyable.

My Comments is an open response area where participants are able to enter their specific comments about the study. Responses may be 1200 characters in length.

APPENDIX G

FIT SCREEN SHOTS

Initial Learning Module Screen Shots

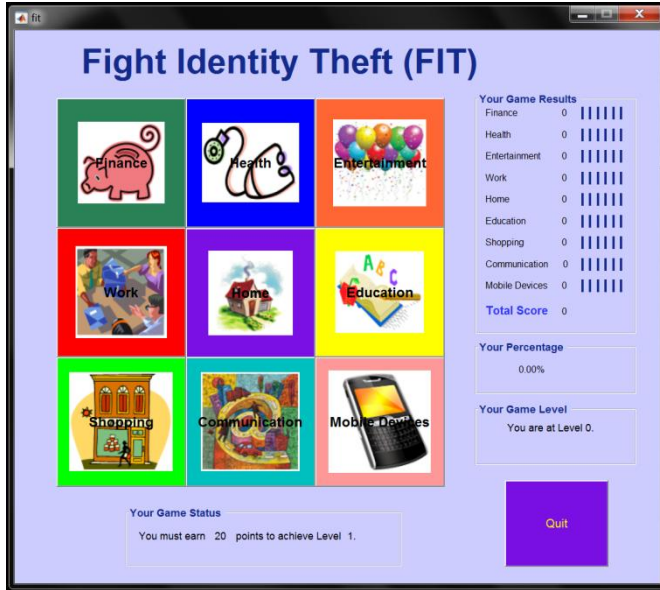


Fig.10.a FIT Game Board Screen

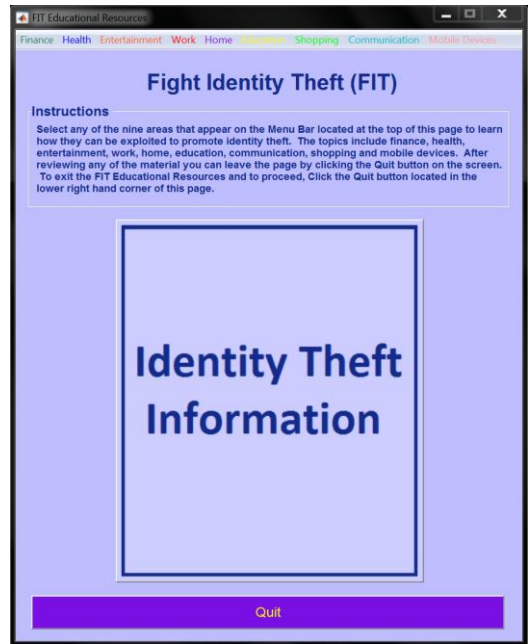


Fig.10.b FIT Text Screen

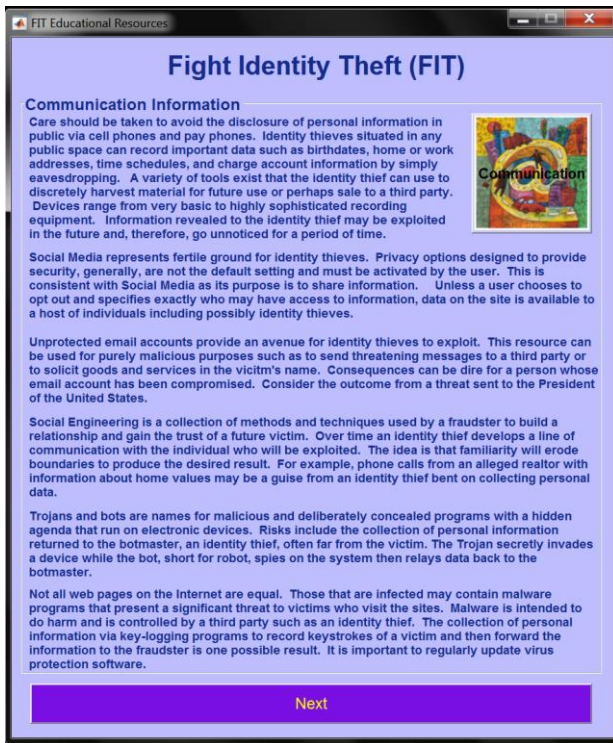


Fig.10.c FIT Text Communication Information



Fig.10d. FIT Text Education Information

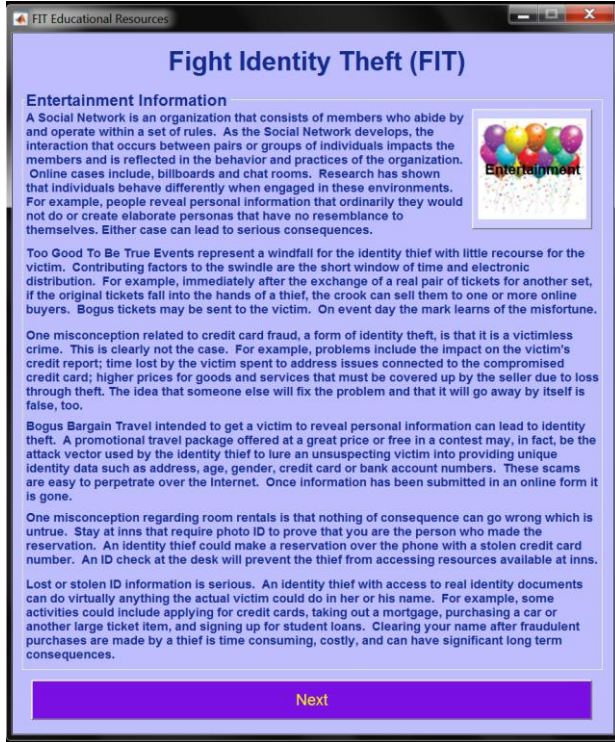


Fig.10.e FIT Text Entertainment Information

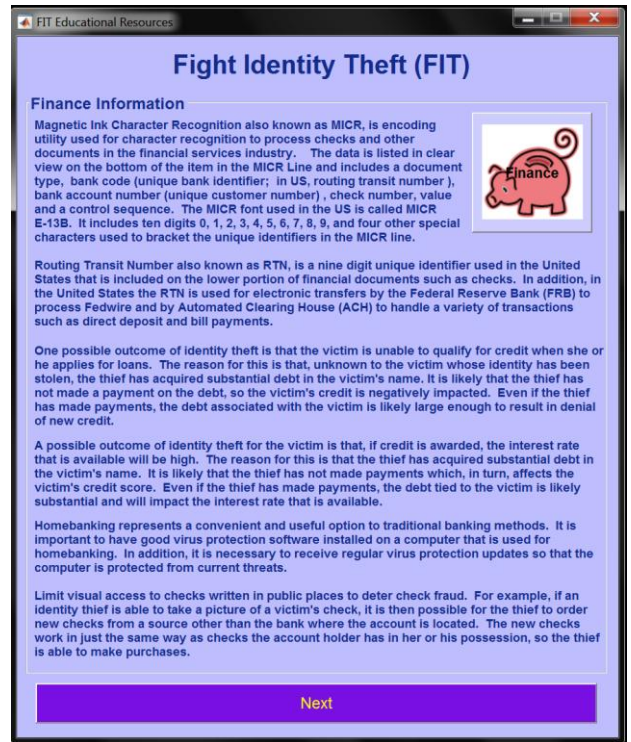


Fig.10.f. FIT Text Finance Information

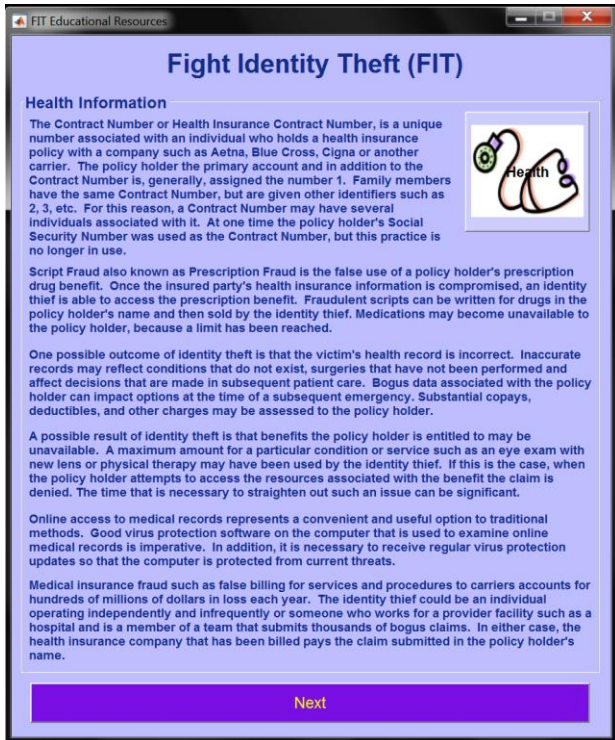


Fig.10.g FIT Text Health Information

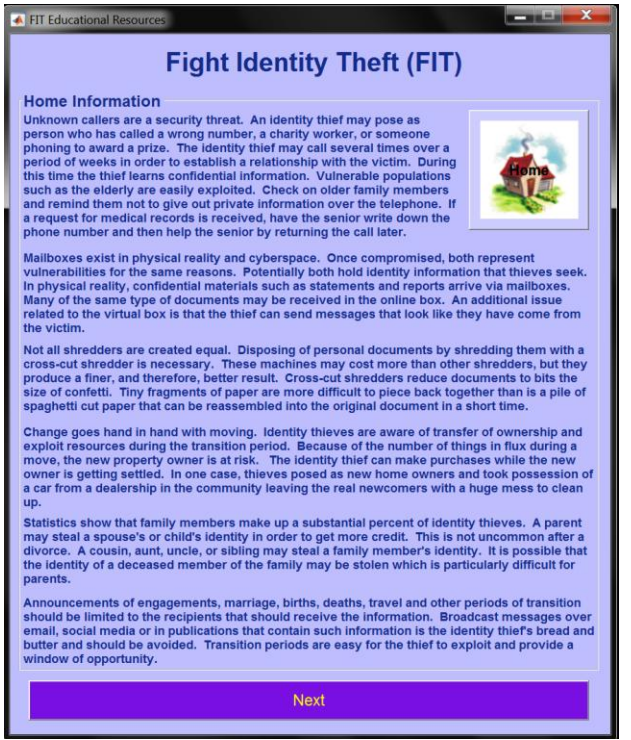



Fig.10.h. FIT Text Home Information

FIT Educational Resources

Fight Identity Theft (FIT)

Mobile Devices Information

War Driving is when an unauthorized user, perhaps an identity thief, accesses an unprotected wireless network for personal gain. The term is derived from the practice of driving a vehicle in search of resources that are available via a private, but open network. The vulnerability could be due to a lack of knowledge on the part of the account holder of Internet settings on the device that is used to connect to the web. The unprotected network allows the war driver to use resources paid for by the victim. For example, large files may be transferred by the thief without the knowledge of the account holder with the resulting data charges billed to the victim.



The majority of current cell phone applications have few or no security features. This is due in part to the fact cell apps have been designed with convenience in mind as the prime focus. Personal information such as addresses or pictures and contact data for friends and family members is readily available to the cell owner, but also is only fingertips away for the identity thief who has walked off with a victim's phone. Keep cell phones in a secure place at all times to avoid data loss.

The majority of current cell phones and a variety of other mobile devices possess weak or no security options. Data stored on them is, therefore, at risk of being compromised by an identity thief who steals the device. Calendars, birthdates, addresses, credit card numbers, passwords, anything saved on the system represents a resource to exploit by an identity thief. The stolen device could also be used to commit fraud in its owner's name which may require countless hours to resolve.

PDA aka Personal Digital Assistant is an acronym used for a host of small hand held devices designed to store user data such as phone numbers, addresses, calendars, passwords and other pieces of information. Devices are often loaded with personal data and are targeted by identity thieves ready to help themselves. The information acquired from a PDA can be used to build bogus accounts based on actual human data which presents a real challenge for law enforcement.

Digital cameras record more than the image that the user wants to save. Unless specific options are disabled, digital cameras also record information such as GPS location data and time a related timestamp. This material may be sensitive, if it leaks information to an identity thief about the photographer's family, schedule, address, habits or other preferences.

Cell phones are small specialized computers and as such are subject to computer viruses just as are larger computer systems. Trojans and other virus programs can steal or corrupt data stored on a cell phone. Substantial quantities of information that identity thieves can exploit is available on cell phones. Thieves target the devices and can access data via electronic transfer with methods similar to those used on other systems.

Next

Fig.10.i FIT Text Mobile Devices Information

FIT Educational Resources

Fight Identity Theft (FIT)

Shopping Information

Misplaced or otherwise out of sight credit cards can affect a credit score, since purchases go through the credit reporting process. Once a card number and authorization code are known to a thief, unauthorized use is possible. For example, if a card leaves the table at a restaurant, information can be recorded for later use. Items can be acquired using the stolen card number without the card through a web application or telephone sale. Purchases made without the owner's consent are often not the responsibility of the card holder, but marks placed on the credit report impact the owner's ability to get credit and rates that are available.



Unauthorized purchases can negatively affect the credit score of the card holder which impacts her or his ability to acquire credit in the future and available interest rates. An identity thief can run up charges on the account owner's credit card. Unpaid balances reflect the indebtedness of the card holder. The greater the debt, the less likely it may be possible to get credit and the higher the lending rate that will be available.

Online scams include the collection of information. A survey may ask a respondent to rate items. Initial questions appear harmless, but later some are slipped in that require personal information such as gender, date of birth or zip code. The sale of items below market value is another technique used to hook victims. A buyer receives goods for a great price, but in doing so must transfer information such as address and credit card to the identity thief.

Unknown charge accounts can negatively affect the credit score of the card holder whose name is associated with it. Bogus accounts can be set up in a victim's name. When card maximums are reached, even if the minimum payment is made by the identity thief, the indebtedness impacts the victim's credit score. Often purchases are for items that can be quickly turned around and sold for cash which makes it difficult to combat this crime.

A compromised checking account occurs when identifiers for an account such as the number, bank identification number and perhaps PIN become known to an identity thief. The crook orders checks with the account owner's account data then receives and uses them. Funds are removed from the owner's account to cover the checks since the bank assumes that they are real.

Providing unnecessary information to another party on the telephone, online or in person puts a person at risk of becoming a victim of identity theft. Information such as date of birth, zip code and gender uniquely identify about 87.5% of the population in the U.S.A. If a seller has no need for a piece of identity information, do not provide it. Thieves assemble data over time. Information collected years earlier can be combined with more recent material to build an identity for future use.

Next


Fig.10.j. FIT Text Shopping Information

FIT Educational Resources

Fight Identity Theft (FIT)

Work Information

Weak passwords represent 25% of all passwords and are a security risk. They offer little protection to the person who selects them and provide the identity thief with access to the individual's resources. Several examples of weak passwords include default passwords set by the manufacture at the factory, birthdates, addresses, hobbies, sports, and names of children or pets. Data that can be learned via online searches and other methods of discovery should be avoided as passwords. Weak passwords can be limited by choosing a combination of letters of both cases, numbers and special characters such as the underscore or ampersand.



Password Sharing eliminates unique access by an individual to resources and services. It represents a substantial security risk, since whoever supplies the correct password enjoys the privileges of the account holder. It is easy for the identity thief to exploit the weakness. A thief offers help to the victim who is having difficulty. The person provides requested login information to the thief who tucks it away for future use after the immediate issue has been addressed.

Unprotected computers which include systems without the latest release of software loaded are a security risk. They can provide identity thieves with access to confidential information. Once an authorized user's account has been compromised, employer data is available to the thief. Virus protection and other software updates from the manufacture should be installed as soon as they are released to limit vulnerabilities related. Corporate espionage is a direct consequence.

Identity thieves posing as visitors or guests from another division of the business are a security threat. Once inside the establishment the thief may be able to access internal networks reserved for employees. They should not be left unsupervised in a room with network connections. The receptionist, secretaries and others who meet the public should receive regular training about guest related procedures. Employees must follow corporate policies established to protect the business.

Resumes should not contain personal and detailed information such as a social security number, references or professional licenses. Reserve this information for the job application. Thieves harvest the data to build identities. The thief posing as a prospective employer requires references that are, in turn, sent to another company where the crook will commit crime in the victim's name.

Personal documents must be handled appropriately. Documents that are to be kept should be stored in a secure manner. Those that are to be discarded should be shredded with a cross-cut shredding machine to reduce the material to tiny pieces. Identity thieves "dumpster dive" or forage in trash piles and receptacles. They collect information and use to construct an identity then exploit resources and leave a mess for the victim to clean up.

Next

Fig.10.k FIT Text Work Information

Sample of One Group of Six Game Questions (Education)

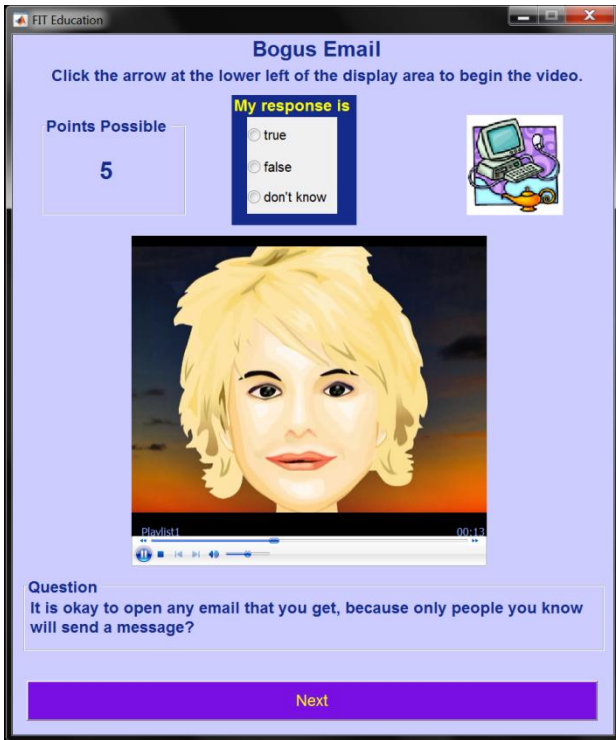


Fig.10.l FIT Game Education Bogus Email

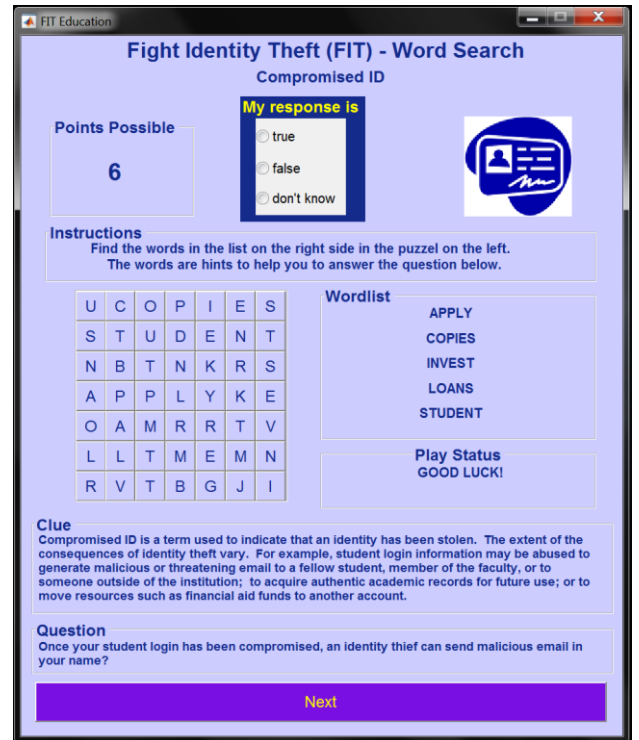


Fig.10.m FIT Game Education Compromised ID - I

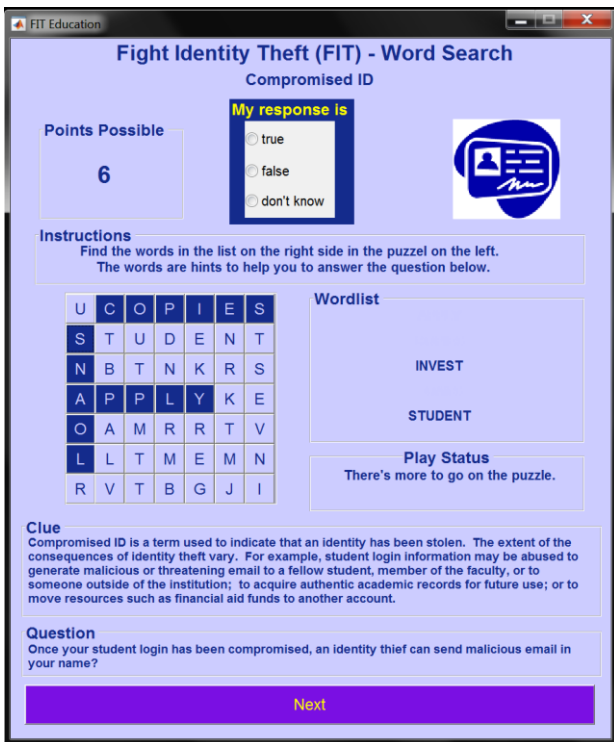


Fig.10.n FIT Game Education Compromised ID - II

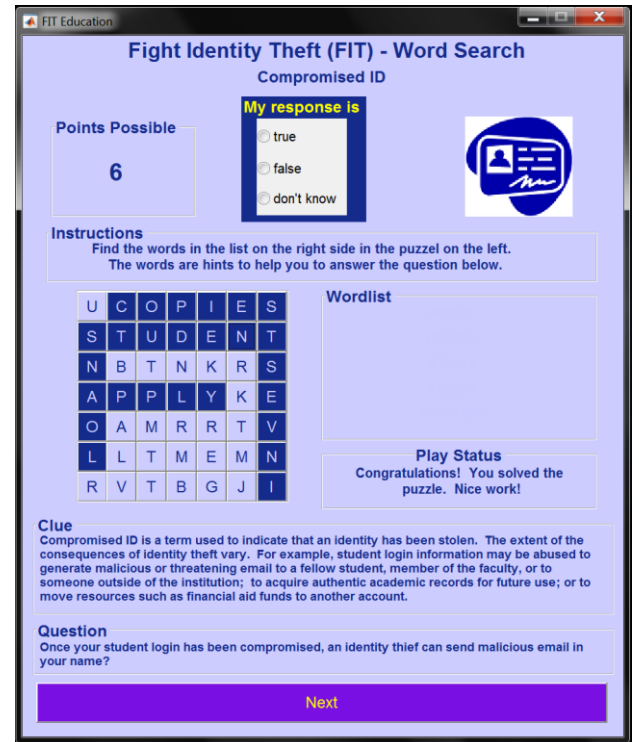


Fig.10.o FIT Game Education Compromised ID - III

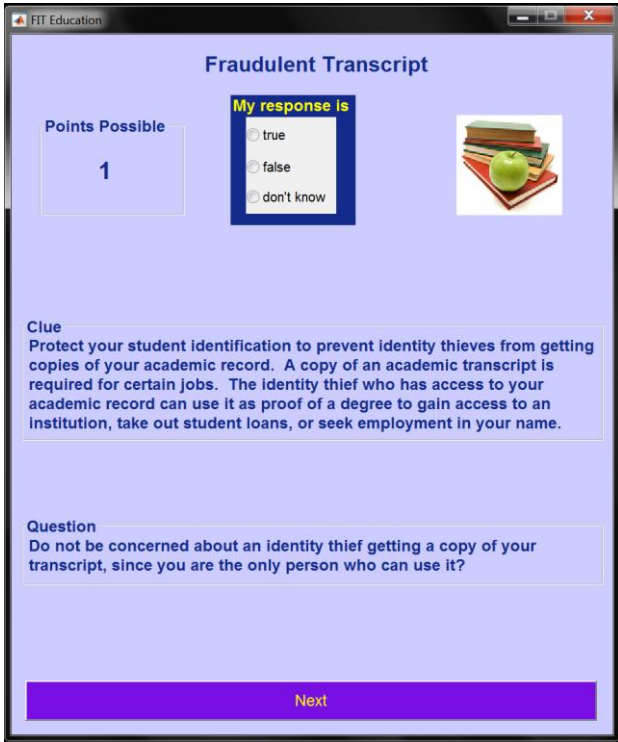


Fig.10.p FIT Game Education Fraudulent Transcript

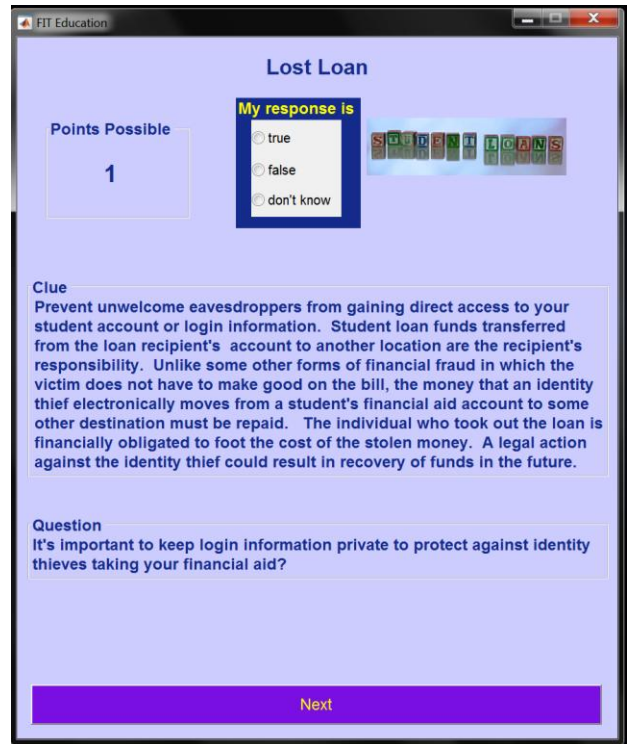


Fig.10.q FIT Game Lost Loan

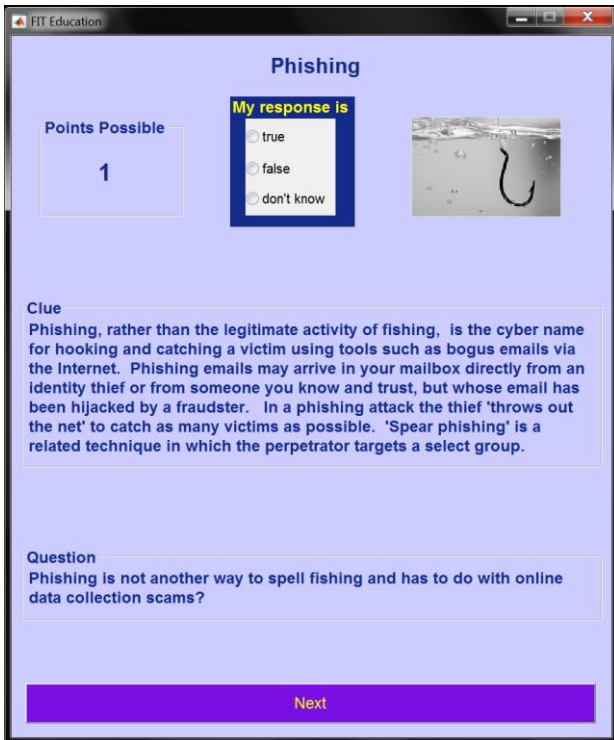


Fig.10.r FIT Game Education Phishing

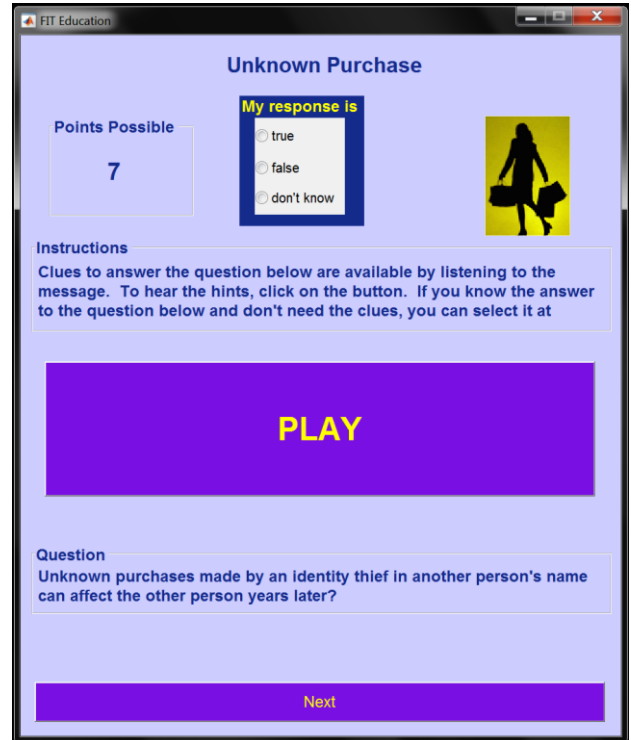


Fig.10.s FIT Game Unknown Purchase

Sample Game Board Intermediate Stages

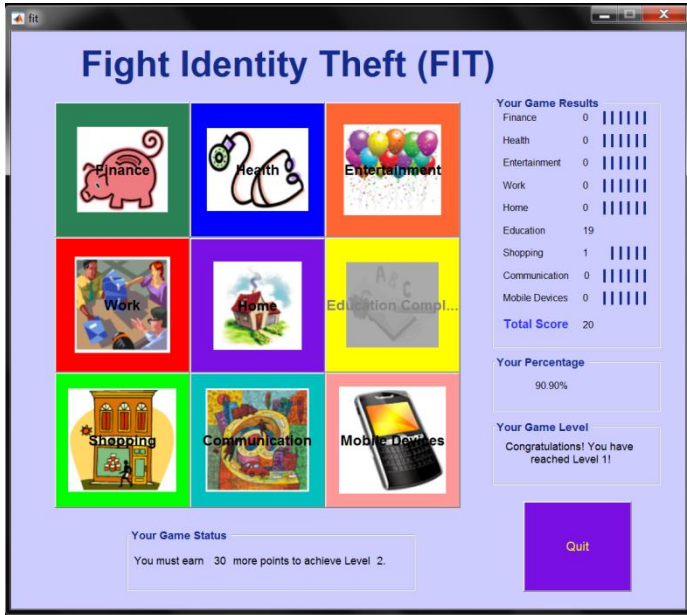


Fig.10.t Game Board Intermediate Screen Shot – I

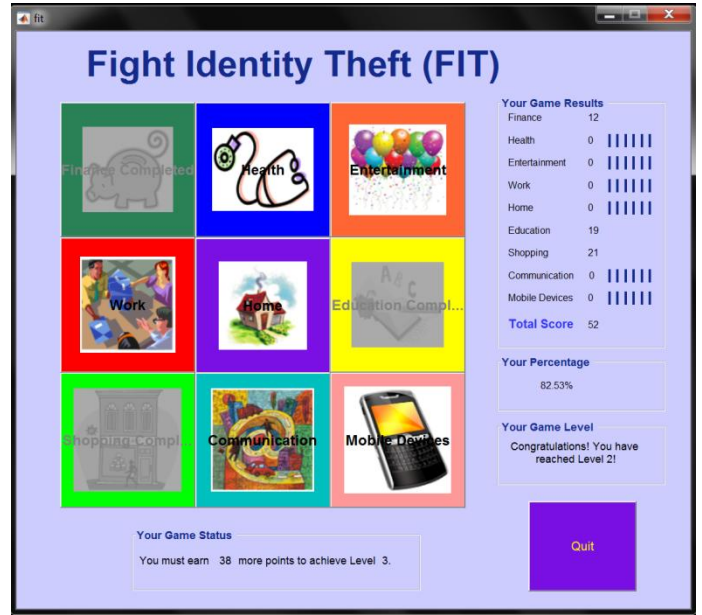


Fig. 10.u Game Board Intermediate Screen Shot - II

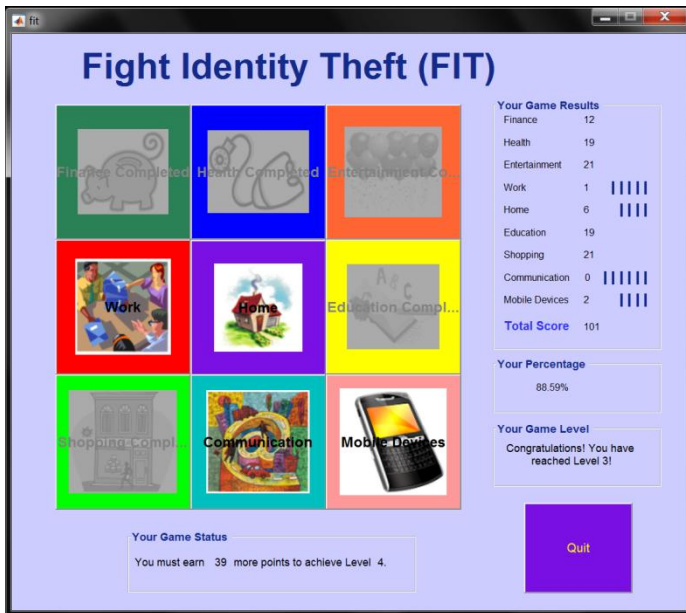


Fig.10.v Game Board Intermediate Screen Shot – III

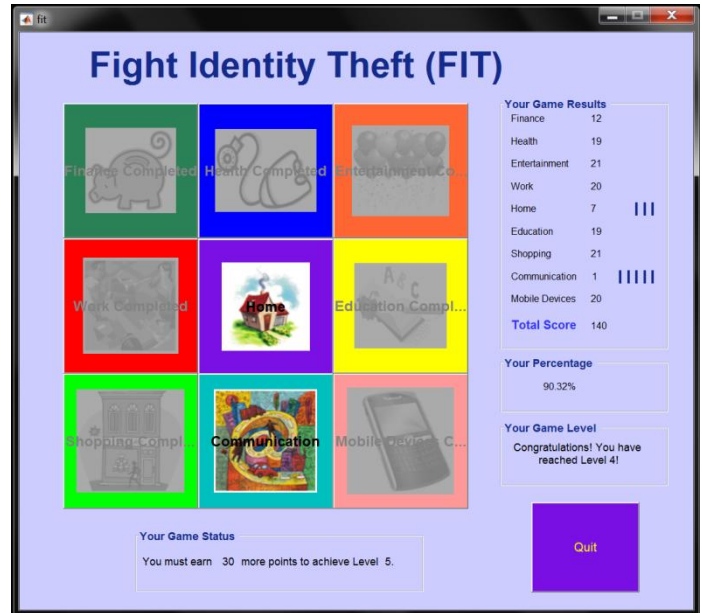


Fig. 10.w Game Board Intermediate Screen Shot - IV

Sample Game Correct and Incorrect Messages

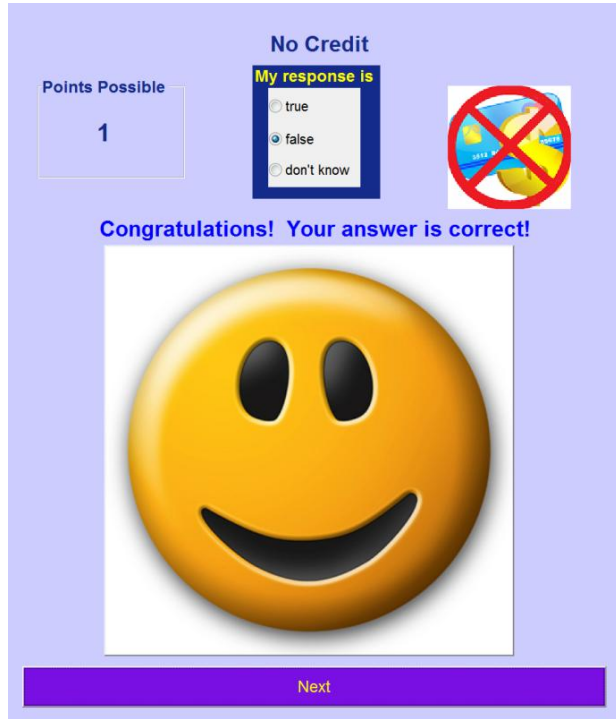


Fig.10.x FIT Game Correct Message

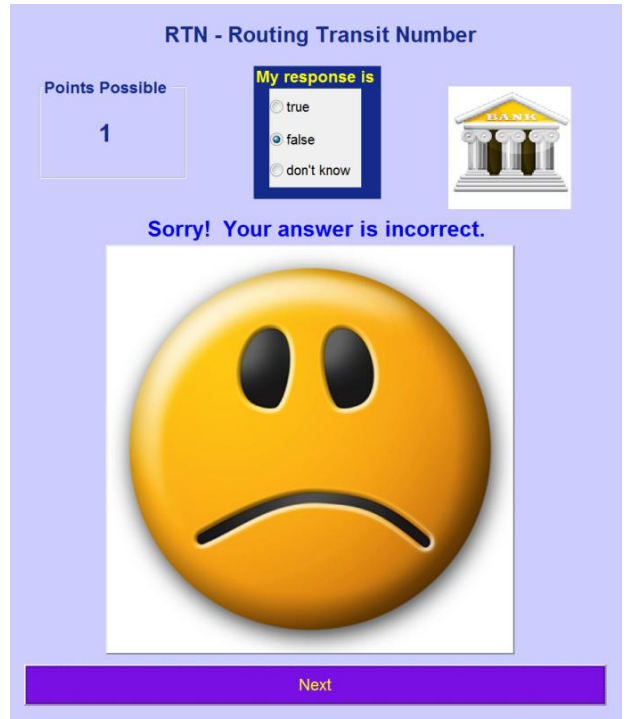


Fig.10.y FIT Game Incorrect Message

FIT Game End Screen and Game or Text Participation Thank You Message

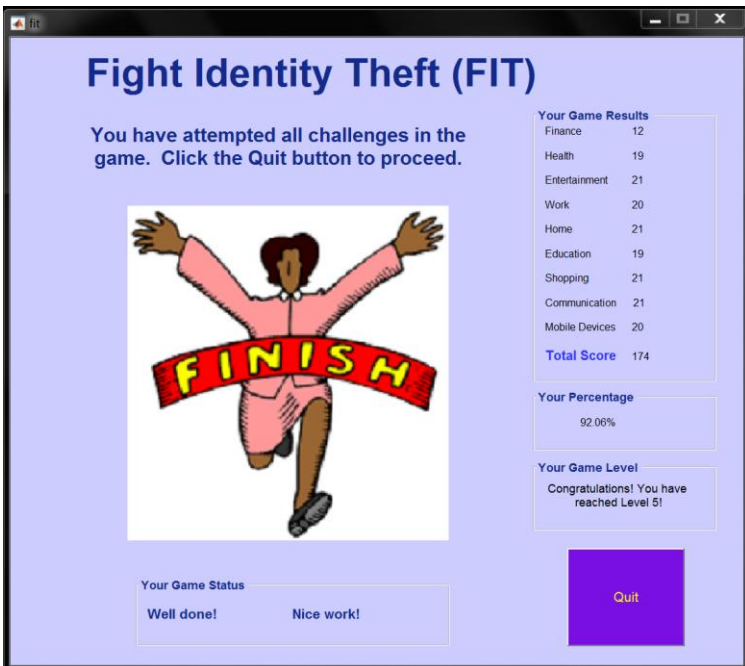


Fig.10.z FIT Game Finish Message

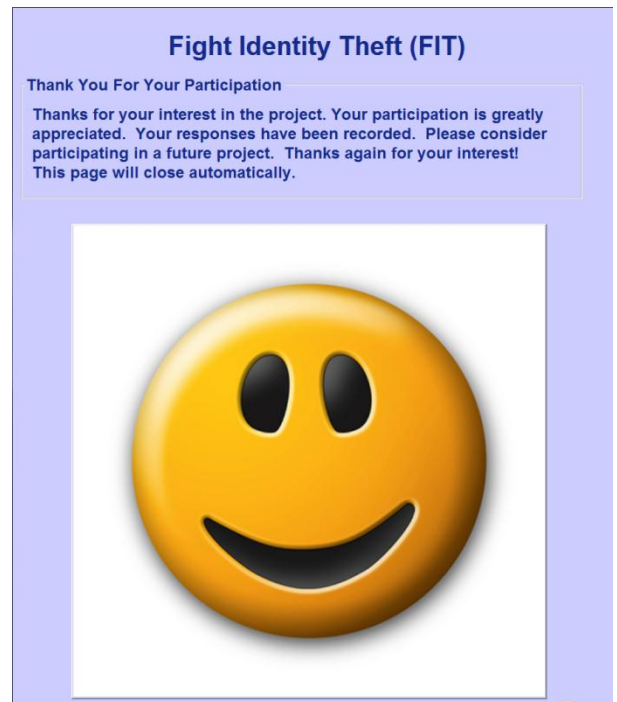


Fig.10.aa FIT Participation Thank You Message

APPENDIX H

FIT APPLICATION FLOW CHART

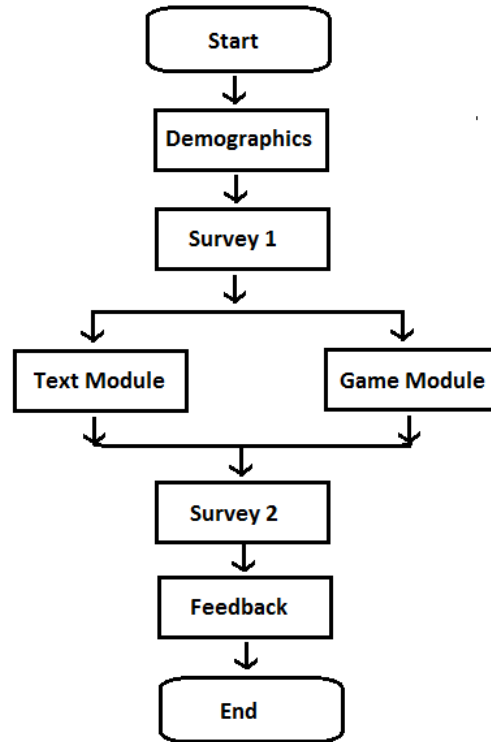


Figure 11: Fight Identity Theft (FIT) Application Flow

APPENDIX I

FIT SURVEY RESPONSE SCORING SYSTEM

Table 3: Scoring System to Assess Movement between Survey 1 (S1) and Survey 2 (S2)

S1 vs. S2	incorrect	don't know	Correct
incorrect	0	1	2
don't know	-1	0	1
correct	-2	-1	0

APPENDIX J

SUMMARY STATISTICS

Table 4: Frequency by Age

Yrs	18 - 22	23 - 30	31 - 45	46 & above
Text	51 (28%)	74 (41%)	37 (21%)	18 (10%)
Game	104 (47%)	66 (30%)	36 (16%)	14 (6%)
Total	155 (39%)	140 (35%)	73 (18%)	32 (8%)

Table 5: Frequency by Gender

Gender	Female	Male
Text	116 (64%)	64 (36%)
Game	147 (67%)	73 (33%)
Total	263 (66%)	137 (34%)

Table 6: Frequency by Technology Savviness

Tech	Low	Low - Med	Med	Med - High	High
Text	17 (9%)	32 (18%)	54 (30%)	58 (32%)	19 (11%)
Game	10 (5%)	52 (24%)	80 (36%)	57 (26%)	21 (10%)
Total	27 (7%)	84 (21%)	134 (34%)	115 (29%)	40 (10%)

Table 7: Frequency by Education

Edu	Some HS	HS Grad	1 Yr Col	2 Yrs Col	More Than 2 Yrs Col
Text	13 (7%)	35 (19%)	59 (33%)	41 (23%)	32 (18%)
Game	21 (10%)	54 (25%)	74 (34%)	35 (16%)	36 (16%)
Total	34 (9%)	89 (22%)	133 (33%)	76 (19%)	68 (17%)

APPENDIX K

SUMMARY SCORES, TIME, AGE, TECH SAVVINESS, EDUCATION

Part I: Text Participants

Table 8: Score & Time

	Score	Time
Avg	1.36	527
Std Dev	1.4	237
Min	-5	36
Max	6	2373
Corr	0.24	

Table 9: Score & Time by Age

	Score	Time	Score	Time	Score	Time	Score	Time
Age	18 – 22		23 – 30		31 -45		46 and greater	
Avg	1.27	508	1.59	561	1.08	477	1.17	544
Std Dev	1.69	143	1.23	328	1.52	117	0.79	173
Min	-5	63	-1	36	-3	136	0	356
Max	5	994	6	2373	4	683	2	1113
Corr	0.23		0.37		0.05		-0.45	

Table 10: Score & Time by Gender

	Score	Time	Score	Time
Gender	female		Male	
Avg	1.36	538	1.34	507
Std Dev	1.52	278	1.17	137
Min	-5	63	-3	36
Max	6	2373	4	814
Corr	0.28		0.06	

Table 11: Score & Time by Tech Savviness

	Score	Time	Score	Time	Score	Time	Score	Time	Score	Time
Tech	Low		Low – Med		Med		Med – High		High	
Avg	1.06	562	1.28	515	1.41	546	1.38	488	1.53	581
Std Dev	1.71	172	1.44	120	1.62	379	1.21	143	0.96	100
Min	-2	359	-2	361	-5	36	-3	92	-1	414
Max	5	1113	5	977	6	2373	4	994	3	814
Corr	0.07		0.43		0.29		0.22		-0.03	

Table 12: Score & Time by Education

	Score	Time	Score	Time	Score	Time	Score	Time	Score	Time
Edu	Some HS		HS Grad		1 Yr Col		2 Yrs Col		More than 2 yrs Col	
Avg	1.15	672	1.49	513	1.17	503	1.37	481	1.47	586
Std Dev	1.91	532	1.4	165	1.49	130	1.16	166	1.29	319
Min	-2	359	0	63	-5	36	0	76	-3	92
Max	6	2373	5	1113	4	831	4	994	3	2199
Corr	0.84		-0.19		0.31		0		0.17	

Part II. Game Participants

Table 13: Scores & Time

	Score	Time
Avg	6.85	1002
Std Dev	3.46	548
Min	-3	40
Max	16	4368
Corr	-0.12	

Table 14: Score & Time by Age

	Score	Time	Score	Time	Score	Time	Score	Time
Age	18 – 22		23 – 30		31 – 45		46 and greater	
Avg	7.63	809	6.35	1151	5.89	1183	6	1262
Std Dev	3.73	631	3.01	405	3.02	356	3.42	418
Min	0	106	-3	40	-3	574	0	619
Max	16	4368	11	2012	10	2038	11	2085
Corr	-0.18		0.35		0.02		-0.21	

Table 15: Score & Time by Gender

	Score	Time	Score	Time
Gender	females		Males	
Ave	6.88	1056	6.78	854
Std Dev	3.43	566	3.56	470
Min	-3	40	0	119
Max	16	4368	16	1808
Corr	-0.14		-0.07	

Table 16: Score & Time by Technology Savviness

	Score	Time	Score	Time	Score	Time	Score	Time	Score	Time
Tech	Low		Low - Med		Med		Med - High		High	
Avg	7.2	869	6.98	1014	6.73	899	6.89	1063	6.76	1263
Std Dev	2.97	669	3.59	486	3.76	645	3.37	439	2.49	417
Min	2	143	0	141	-3	40	0	119	0	122
Max	13	1906	16	1804	14	4368	14	2132	10	2085
Corr	0.23		-0.2		-0.07		-0.2		-0.3	

Table 17: Score & Time by Education

	Score	Time	Score	Time	Score	Time	Score	Time	Score	Time
Edu	Some HS		HS Grad		1 Yr		2 Yrs		More than 2	
Avg	5.81	1079	7.13	898	7.66	971	6.23	976	6	1200
Std Dev	2.62	548	3.9	559	3.65	658	3.05	421	2.79	312
Min	0	118	-3	106	-3	108	0	40	0	757
Max	10	1906	16	2012	16	4368	10	2132	10	2085
Corr	0.24		-0.07		-0.24		0.27		-0.26	

APPENDIX L

SUMMARY SCORES, TIME, BENEFIT, ENJOYMENT

Part I:

Table 18: Benefit Level

Ben	No Op	None	Low	Mod	High
Text	93 (52%)	52 (29%)	33 (18%)	2 (1%)	0 (0%)
Game	20 (9%)	1 (1%)	24 (11%)	50 (23%)	125 (57%)

Table 19: Enjoyment Level

Enjoy	No Op	None	Low	Mod	High
Text	56 (31%)	19 (11%)	89 (49%)	15 (8%)	1 (1%)
Game	19 (9%)	1 (1%)	30 (14%)	54 (25%)	116 (53%)

Part II: Text

Table 20: Overall Benefit & Enjoyment

	Ben	Enjoy
Avg	1.69	2.37
Std Dev	0.81	1.03
Min	1	1
Max	4	5

Table 21: Benefit Level

	Score	Time	Score	Time	Score	Time	Score	Time	Score	Time
Ben	No Op		None		Low		Mod		High	
Avg	1.31	514.9	1.02	501.55	1.97	593.07	2	665.17	NA	NA
Std Dev	1.34	224.56	1.46	151.01	1.36	353.76	0	209.81	NA	NA
Min	-2	64	-5	148	-1	36	2	517	0	0
Max	5	2199	3	1113	6	2373	2	814	0	0
Corr	0.06		0.18		0.56		NA		NA	

Table 22: Enjoyment Level

	Score	Time	Score	Time	Score	Time	Score	Time	Score	Time
Enjoy	No Op		None		Low		Mod		High	
Avg	1.2	448.41	0.37	586.75	1.58	534.71	2	593.36	3	976.96
Std Dev	1.35	138.4	2.24	467.78	1.24	272.78	1	113.82	NA	NA
Min	-2	64	-5	186	-2	36	0	380	3	977
Max	5	669	6	2373	5	2199	4	814	3	977
Corr	-0.22		0.62		0.12		0.47		NA	

Table 23: Sample Qualitative Feedback

	Sample of Comments
1	I didn't know identity theft messes up insurance.
2	I knew the answers to the questions the 1st time
3	I'm in this field and learned a few things. Anywhere you learn something is worthwhile.
4	It was ok
5	Lots to think about.
6	print is to small
7	There is good information. It is a lot to absorb at once.
8	This is important material.
9	to much to read
10	why cant I go to the info wheni do the questions?

Part III: Game

Table 24: Overall Benefit & Enjoyment

	Ben	Enjoy
Avg	4.18	4.12
Std Dev	1.22	1.2
Min	1	1
Max	5	5

Table 25: Benefit Level

	Score	Time	Score	Time	Score	Time	Score	Time	Score	Time
Ben	No Op		None		Low		Mod		High	
Avg	5.9	538.71	0	138.49	8.13	650.55	7.24	761.71	6.66	1246.21
Std Dev	5.18	514.41	NA	NA	4.68	933.81	3.78	365.52	2.52	357.97
Min	-3	40	0	139	-3	108	0	118	0	151
Max	14	1796	0	139	16	4368	16	1527	11	2132
Corr	-0.17		NA		-0.03		-0.23		-0.15	

Table 26: Enjoyment Level

	Score	Time	Score	Time	Score	Time	Score	Time	Score	Time
Enjoy	No Op		None		Low		Mod		High	
Avg	6.37	530.29	0	138.49	7.87	653.9	6.89	821.07	6.72	1260.5
Std Dev	4.87	527.09	NA	NA	4.62	800.45	3.95	446.59	2.4	343.7
Min	0	40	0	138	-3	108	0	118	0	151
Max	14	1796	0	139	16	4368	16	2038	11	2132
Corr	-0.16		NA		0.01		-0.36		-0.06	

Table 27: Sample Qualitative Feedback

	Sample of Comments
1	Awsome! Excellent way to learn about identity theft. This is really useful.
2	Clues are good. I missed some answers. I shoulda done all clues.
3	E/I - Educational and Informational - Also, Enjoyable. Good combo of activities. It held my interest.
4	Have lots of high point questions.
5	I got to level 3. I needed more time to get a higher score.
6	I would like to pick questions by their points
7	some of the videos are to long
8	Thanx
9	This a good way to learn about identity theft. Sound could be louder on some panels.
10	videos, soud & games are best

Part IV:

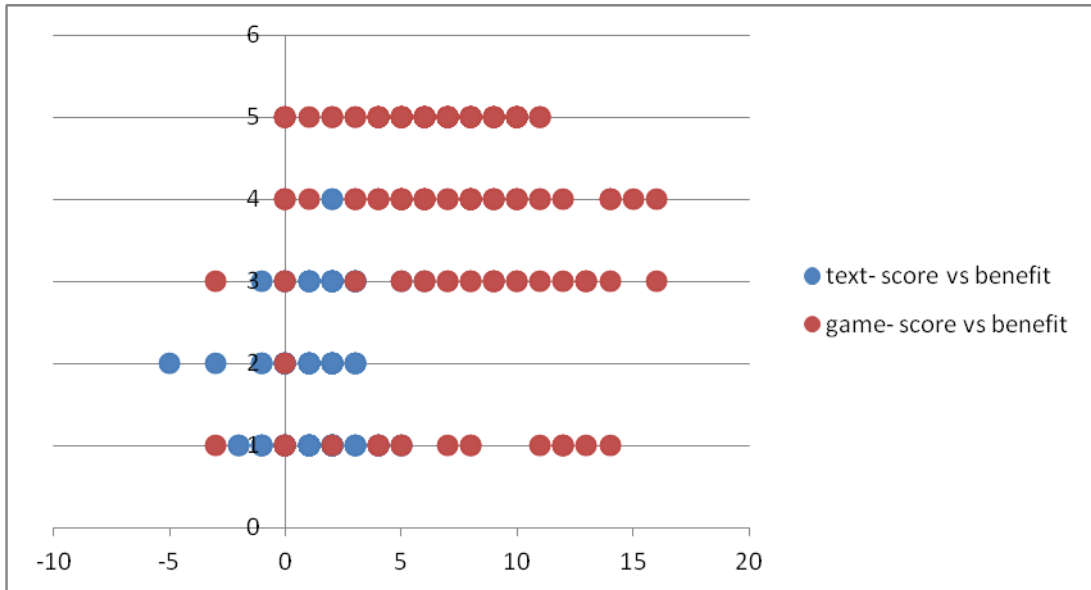


Figure 12: Frequency Score vs Benefit

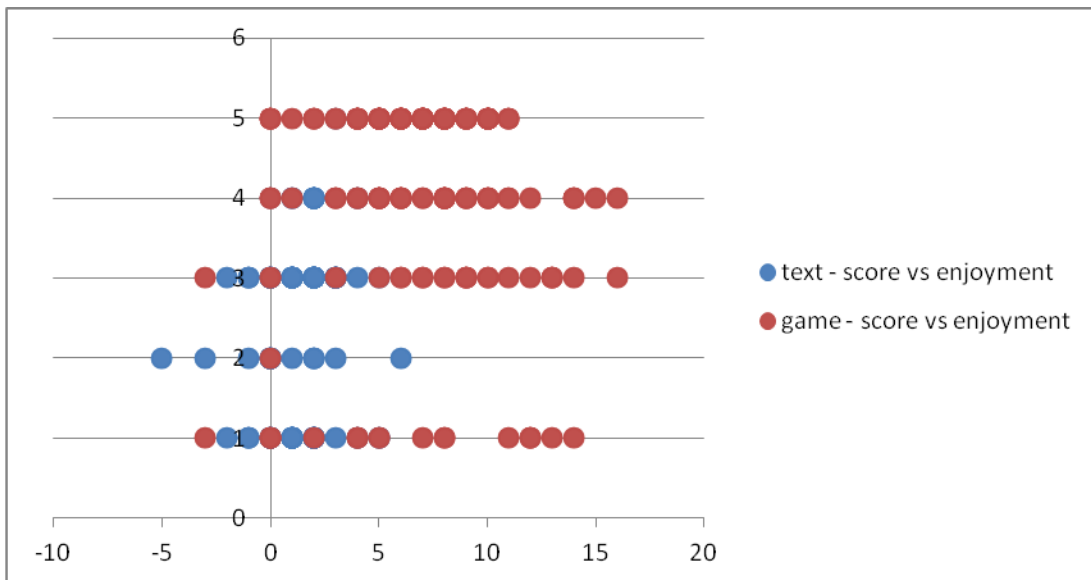


Figure 13: Frequency Score vs Enjoyment

APPENDIX M

CHANGES IN THE PARTICIPANTS' SCORES ON SURVEYS

Table 28: Participant Response Change Key

	Indicates significant difference in Incorrect/Incorrect for Text- & Game-Based
	Indicates significant difference in "Don't Know"/"Don't Know" for Text- & Game-Based
	Indicates significant difference in Incorrect/Correct for Text- & Game-Based
	Indicates significant difference in "Don't Know"/Correct for Text- & Game-Based
	Indicates significant difference in Incorrect/"Don't Know" for Text- & Game-Based

Table 29: Question 1: Identity theft can lead to credit problems

Q1	Txt			Game		
	Incorrect	Don't Know	Correct	Incorrect	Don't Know	Correct
Incorrect	33 (18%)	18 (10%)	4 (2%)	8 (4%)	12 (6%)	53 (24%)
Don't Know	3 (2%)	51 (28%)	13 (7%)	3 (1%)	3 (1%)	82 (37%)
Correct	1 (1%)	2 (1%)	55 (31%)	0 (0%)	0 (0%)	59 (27%)

Table 30: Question 2: Medical insurance can be denied, because of identity theft

Q2	Txt			Game		
	Incorrect	Don't Know	Correct	Incorrect	Don't Know	Correct
Incorrect	29 (16%)	17 (9%)	13 (7%)	6 (3%)	14 (6%)	56 (26%)
Don't Know	7 (4%)	48 (27%)	8 (4%)	4 (2%)	7 (3%)	83 (38%)
Correct	1 (1%)	2 (1%)	55 (31%)	1 (1%)	0 (0%)	49 (22%)

Table 31: Question 3: It is smart to buy from the cheapest online vendor

Q3	Txt			Game		
Frequency & %	Incorrect	Don't Know	Correct	Incorrect	Don't Know	Correct
Incorrect	43 (24%)	7 (4%)	4 (2%)	9 (4%)	40 (18%)	28 (13%)
Don't Know	1 (1%)	54 (30%)	8 (4%)	5 (2%)	11 (5%)	61 (28%)
Correct	0 (0%)	3 (2%)	60 (33%)	0 (0%)	2 (1%)	64 (29%)

Table 32: Question 4: Phishing can occur at work

Q4	Txt			Game		
Frequency & %	Incorrect	Don't Know	Correct	Incorrect	Don't Know	Correct
Incorrect	26 (14%)	34 (19%)	8 (4%)	6 (3%)	25 (11%)	31 (14%)
Don't Know	6 (3%)	45 (25%)	12 (7%)	7 (3%)	10 (5%)	79 (36%)
Correct	1 (1%)	2 (1%)	46 (26%)	0 (0%)	3 (1%)	59 (27%)

Table 33: Question 5: Social engineering is a form of social media

Q5	Txt			Game		
Frequency & %	Incorrect	Don't Know	Correct	Incorrect	Don't Know	Correct
Incorrect	50 (28%)	12 (7%)	3 (2%)	4 (2%)	44 (20%)	29 (13%)
Don't Know	2 (1%)	44 (24%)	6 (3%)	3 (1%)	22 (10%)	54 (25%)
Correct	1 (1%)	2 (1%)	60 (33%)	0 (0%)	2 (1%)	62 (28%)

Table 34: Question 6: It's okay to stay logged on to a computer when you leave it for a few minutes

Q6	Txt			Game		
Frequency & %	Incorrect	Don't Know	Correct	Incorrect	Don't Know	Correct
Incorrect	37 (21%)	13 (7%)	5 (3%)	7 (3%)	44 (20%)	39 (18%)
Don't Know	1 (1%)	46 (26%)	14 (8%)	2 (1%)	13 (6%)	54 (25%)
Correct	1 (1%)	2 (1%)	61 (34%)	0 (0%)	1 (1%)	60 (27%)

Table 35: Question 7: Purchases that you don't make don't impact your credit

Q7	Txt			Game		
	Incorrect	Don't Know	Correct	Incorrect	Don't Know	Correct
Incorrect	43 (24%)	5 (3%)	4 (2%)	7 (3%)	37 (17%)	30 (14%)
Don't Know	1 (1%)	58 (32%)	13 (7%)	7 (3%)	11 (5%)	68 (31%)
Correct	1 (1%)	2 (1%)	53 (29%)	1 (1%)	5 (2%)	54 (25%)

Table 36: Question 8: Social media sites are good places to share your information

Q8	Txt			Game		
	Incorrect	Don't Know	Correct	Incorrect	Don't Know	Correct
Incorrect	56 (31%)	6 (3%)	2 (1%)	9 (4%)	48 (22%)	38 (17%)
Don't Know	2 (1%)	45 (25%)	5 (3%)	3 (1%)	8 (4%)	50 (23%)
Correct	1 (1%)	2 (1%)	61 (34%)	0 (0%)	1 (1%)	63 (29%)

Table 37: Question 9: Cell apps are reliable

Q9	Txt			Game		
	Incorrect	Don't Know	Correct	Incorrect	Don't Know	Correct
Incorrect	55 (31%)	16 (9%)	1 (1%)	6 (3%)	48 (22%)	28 (13%)
Don't Know	1 (1%)	46 (26%)	10 (6%)	3 (1%)	16 (7%)	60 (27%)
Correct	0 (1%)	6 (3%)	45 (25%)	1 (1%)	2 (1%)	56 (26%)

APPENDIX N

CALCULATED SCORES, FREQUENCIES AND PERCENTS

Table 38: Calculated Scores, Frequencies & Percents

Score	Txt		Game	
	Freq	Pct	Freq	Pct
-18	0	0	0	0
-17	0	0	0	0
-16	0	0	0	0
-15	0	0	0	0
-14	0	0	0	0
-13	0	0	0	0
-12	0	0	0	0
-11	0	0	0	0
-10	0	0	0	0
-9	0	0	0	0
-8	0	0	0	0
-7	0	0	0	0
-6	0	0	0	0
-5	1	1	0	0
-4	0	0	0	0
-3	1	1	2	1
-2	2	1	0	0
-1	7	4	0	0
0	34	19	15	7
1	45	25	2	1
2	66	37	4	2
3	15	8	6	3
4	5	3	15	7
5	3	2	26	12
6	1	1	26	12
7	0	0	28	13
8	0	0	33	15
9	0	0	16	7
10	0	0	23	11

11	0	0	7	3
12	0	0	5	2
13	0	0	4	2
14	0	0	5	2
15	0	0	1	1
16	0	0	2	1
17	0	0	0	0
18	0	0	0	0

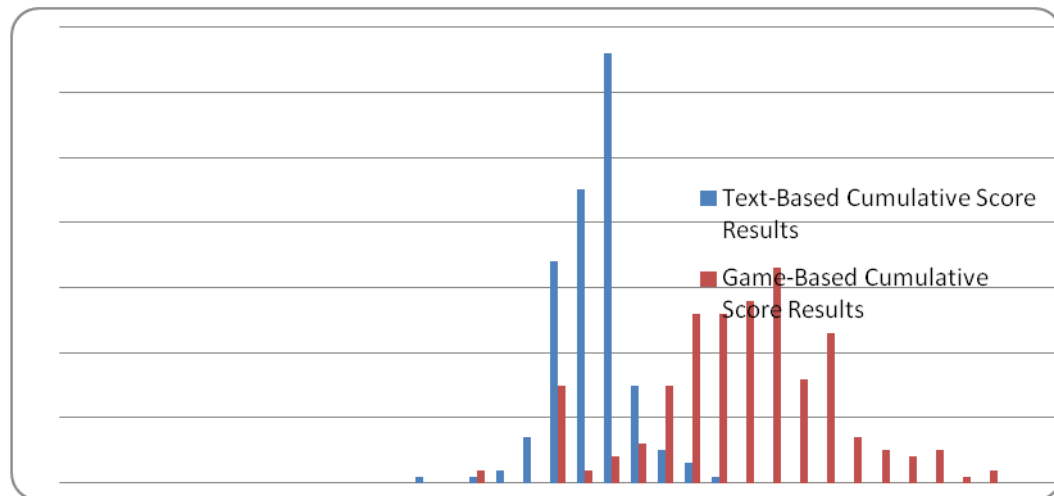


Figure 14: Cumulative Score Results for Text-Based and Game-Based Modules

APPENDIX O

GROUPED QUESTIONS RESULTS 127, 368, 459

Table 39a: Key to 39b

	Worsen: DI CD, CI
	No Change: II, DD
	Improve: ID, IC, DC
	Similar: *
	Behavior: CI, CD, CC

Table 39b: Grouped Questions Data (127; 368; 459)

Text						Groups	Game					
Imp	Wor	NC	Sim	CI/CD	CC		Imp	Wor	NC	Sim	CI/CD	CC
28%	5%	67%	*			1	91%	2%	7%	*		
30%	8%	62%	*	5%	95%	2	89%	3%	8%	*	4%	96%
18%	3%	79%				7	81%	8%	11%			
16%	3%	81%	*			3	83%	4%	13%	*		
27%	3%	69%		5%	95%	6	86%	2%	13%	*	2%	98%
11%	4%	85%	*			8	87%	3%	11%	*		
40%	7%	53%				4	84%	6%	10%	*		
18%	4%	78%	*	7%	93%	5	84%	6%	10%	*	4%	96%
20%	5%	75%	*			9	83%	4%	13%	*		

APPENDIX P
RESEARCH DATA

Table 40: Text Data

a g e	g e n d e r	t e c h	e d u	S 1 1	S 1 2	S 1 3	S 1 4	S 1 5	S 1 6	S 1 7	S 1 8	S 1 9	S 2 1	S 2 2	S 2 3	S 2 4	S 2 5	S 2 6	S 2 7	S 2 8	S 2 9	b e n e	e n j	t l m e	s c o r e
3	1	3	1	2	2	2	2	2	2	2	2	2	0	0	0	0	0	0	0	0	0	3	2	2373	6
2	1	3	3	1	1	1	1	1	1	1	1	1	1	0	1	1	2	2	2	2	1	2	2	186	-5
2	1	2	2	1	0	2	1	2	2	1	2	2	1	2	0	1	2	2	1	2	1	3	3	552	5
2	1	1	2	0	0	2	1	2	2	1	2	1	0	2	2	1	2	0	0	2	1	1	1	456	5
2	2	3	3	1	1	2	1	2	2	1	0	1	1	1	2	1	2	0	1	1	0	2	3	462	2
4	2	4	4	1	1	0	1	1	2	1	0	2	2	1	0	2	1	0	1	0	2	1	1	372	4
2	2	3	3	1	1	2	1	2	2	0	2	1	1	0	2	1	1	2	1	2	1	2	3	477	-1
2	1	4	3	2	2	0	0	1	0	1	0	1	2	2	0	2	1	0	1	0	1	1	3	442	2
5	1	3	3	2	1	2	1	1	1	0	0	1	2	1	2	2	1	0	0	0	1	2	3	356	2
2	2	4	3	1	1	2	1	2	1	1	2	1	1	1	2	1	1	0	1	2	1	2	2	472	2
3	2	3	3	2	0	0	2	0	2	1	0	0	2	0	0	2	0	0	1	0	0	2	1	569	2
2	2	3	2	0	0	1	0	0	0	2	1	0	0	0	1	1	1	0	2	0	0	2	3	491	1
3	2	3	2	1	1	2	1	1	2	1	1	2	1	1	2	0	1	1	1	1	1	1	1	302	1
2	1	5	4	2	0	2	1	1	1	1	0	1	2	0	2	1	1	1	1	0	0	1	1	413	1
2	1	4	4	2	0	1	1	2	1	2	1	1	2	2	1	1	2	0	2	1	1	3	3	994	3
5	1	2	2	2	2	0	2	0	2	1	2	2	2	2	0	2	0	2	1	2	1	2	2	393	1
4	2	4	3	2	2	0	2	0	0	0	2	0	2	2	0	2	0	0	0	2	0	1	2	488	0
4	1	2	2	2	2	1	2	1	1	2	2	2	2	2	1	2	0	1	1	2	2	2	4	600	2
2	1	1	1	1	1	0	1	1	0	2	0	1	1	0	0	0	1	0	2	0	1	1	3	517	-2
3	1	2	2	0	2	0	1	1	1	1	1	1	0	2	0	1	1	1	0	1	1	3	3	454	1
5	1	4	4	0	1	0	0	0	1	1	2	0	0	1	0	1	0	0	1	2	0	2	3	372	2
5	2	5	5	2	2	0	0	1	1	1	1	2	2	2	0	0	1	1	1	0	1	2	3	554	2
4	1	2	2	0	0	1	0	2	0	0	2	2	0	0	1	0	2	0	0	2	2	2	2	594	0
2	1	1	1	1	0	0	2	0	0	0	1	2	0	1	1	2	0	0	0	1	1	2	3	478	0
3	2	3	3	2	0	0	0	0	0	1	2	1	2	0	0	0	0	0	0	2	1	2	3	554	1
3	2	5	4	0	2	2	1	1	1	1	0	2	0	2	2	1	0	0	1	0	2	2	3	432	2
4	2	4	3	0	1	0	1	0	2	0	1	2	0	1	0	1	0	2	0	1	1	1	1	509	1
3	1	2	2	0	2	1	0	0	1	2	1	1	0	2	1	1	0	0	2	1	1	3	3	516	2
3	1	3	3	2	2	1	0	1	1	0	0	1	2	2	0	0	1	1	0	0	1	2	3	711	1

3	1	3	3	2	2	0	2	0	0	1	1	1	2	2	0	2	0	0	1	1	1	1	2	542	0
3	1	3	4	1	1	0	0	2	0	2	1	0	0	1	1	2	1	1	0	1	1	2	3	479	1
4	2	4	5	1	1	0	0	0	1	0	0	1	2	2	0	0	0	1	0	0	1	1	3	619	2
3	2	3	2	2	1	0	2	1	0	0	0	0	2	2	0	2	0	0	2	0	0	3	4	380	0
5	2	5	5	2	2	0	2	0	0	0	0	0	2	2	0	2	0	0	0	0	0	1	3	695	0
2	1	3	3	0	0	0	1	2	2	1	0	0	1	1	0	1	2	2	1	0	0	1	3	490	2
4	2	4	4	2	0	2	1	1	2	2	0	2	2	0	2	1	1	2	2	0	1	2	3	440	1
3	2	3	3	1	1	2	1	0	1	0	0	0	1	1	2	1	0	1	0	0	0	2	1	485	0
3	2	1	2	0	1	1	2	0	1	2	1	2	0	1	1	2	0	1	2	0	1	2	3	705	2
2	1	2	2	0	1	1	0	0	1	1	0	2	1	1	1	1	0	1	1	0	2	2	1	459	2
2	1	1	1	0	1	1	0	2	1	0	2	0	1	1	1	0	2	1	0	2	1	1	3	359	0
3	1	2	3	0	1	2	1	1	1	2	2	1	1	1	2	1	1	1	2	2	1	1	1	448	1
4	2	4	4	1	0	0	2	2	1	2	1	0	1	0	0	2	2	1	2	1	0	2	3	357	0
3	2	4	4	0	2	0	2	0	2	0	1	1	0	2	0	2	0	2	0	1	1	1	1	295	0
4	2	3	3	2	2	0	2	0	2	1	1	2	2	2	0	2	0	2	1	1	2	2	2	348	0
3	2	4	2	1	0	2	2	2	1	0	1	1	1	0	2	2	1	0	0	1	0	2	2	462	3
5	1	2	3	0	0	1	0	2	2	2	1	0	0	0	1	1	2	2	2	1	1	1	3	395	0
3	1	3	4	1	2	1	0	0	2	2	0	1	1	2	1	2	0	1	2	0	1	1	3	353	3
2	2	4	4	0	1	1	2	2	2	1	1	2	0	1	1	2	2	2	0	1	2	1	1	392	1
3	1	3	3	0	0	1	2	1	1	1	2	2	0	0	0	2	1	1	1	2	2	2	1	387	1
3	1	3	3	0	1	2	1	1	2	1	0	0	0	1	2	1	1	2	1	0	0	1	1	478	0
2	1	1	1	2	1	1	2	0	0	2	2	0	2	1	1	2	0	0	2	2	0	2	2	429	0
2	1	2	2	2	0	2	1	0	0	0	2	1	2	0	2	1	0	0	0	2	1	1	1	368	0
3	2	4	3	0	0	2	1	0	2	2	1	1	0	0	2	0	0	1	2	1	1	2	2	544	0
2	1	2	2	1	2	2	0	2	1	1	1	2	1	2	2	0	2	1	1	1	2	1	1	418	0
3	1	3	4	2	2	2	0	2	2	1	2	2	2	2	0	2	2	1	2	2	2	3	508	0	
4	2	3	4	0	2	1	1	2	0	0	2	2	1	2	1	1	2	0	0	2	2	2	3	487	1
2	2	4	3	2	1	1	1	0	2	0	0	2	2	1	1	1	0	2	0	0	2	1	1	350	0
3	1	3	4	1	0	0	1	0	0	2	2	0	1	2	0	1	0	0	2	2	0	2	3	410	2
4	2	4	4	0	0	1	1	0	2	1	2	1	0	0	0	2	0	2	1	2	1	2	1	148	2
4	2	4	4	0	1	0	1	1	0	0	1	1	0	1	0	1	1	0	0	1	1	1	1	507	0
2	1	2	2	0	0	0	1	1	0	1	1	0	0	0	0	1	1	0	0	1	0	2	3	508	1
3	2	4	4	2	2	0	0	0	1	0	2	1	2	2	0	1	0	1	0	2	1	1	3	380	1
3	1	3	4	1	1	1	2	1	1	1	0	1	1	1	1	2	0	1	0	0	1	1	3	541	2
2	2	5	3	1	0	0	2	0	0	1	1	2	1	0	0	2	0	0	1	1	1	1	3	574	1
3	1	4	4	1	2	0	2	0	0	0	1	2	1	2	0	2	0	0	0	1	2	2	2	423	0
3	2	4	5	0	1	1	1	0	0	1	2	2	1	1	0	1	0	0	1	2	2	2	3	576	2
3	1	2	2	1	2	1	1	1	1	2	1	0	1	2	1	1	1	1	2	1	0	2	2	361	0
4	1	2	3	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	2	1	1	1	404	0
4	1	3	3	2	2	0	2	1	0	0	0	2	2	2	0	2	1	0	0	0	2	1	1	349	0
4	2	4	3	0	1	1	1	0	0	0	0	1	0	1	1	1	0	0	0	0	1	1	3	414	0

4	1	3	2	0	2	1	0	0	1	1	0	0	0	2	1	0	0	1	1	0	0	2	2	468	0
3	2	4	3	1	1	2	0	1	2	2	2	1	1	1	2	0	1	2	2	1	0	1	2	415	2
3	2	4	3	0	0	0	1	2	2	2	0	1	1	1	0	1	2	2	2	0	1	1	3	743	2
3	1	4	5	0	1	2	0	0	2	0	0	2	0	1	2	1	0	2	0	0	2	1	3	437	1
2	1	4	4	1	2	0	0	0	0	2	2	2	1	2	0	0	0	2	0	2	2	2	2	452	2
4	1	3	3	2	2	2	2	2	1	0	2	2	2	2	2	2	1	1	0	2	2	2	1	433	1
3	2	4	3	0	2	0	1	1	0	2	1	0	1	2	0	2	1	0	2	1	0	3	3	408	2
4	1	3	5	1	0	1	2	0	2	1	0	2	1	1	1	2	0	2	1	0	1	3	3	397	2
4	1	5	5	1	1	0	0	0	1	0	1	2	1	1	0	2	0	1	0	1	1	2	3	534	3
2	1	4	3	1	2	0	0	1	2	2	0	2	1	2	0	2	1	2	2	0	2	3	3	496	2
3	2	2	3	2	0	1	2	2	2	0	2	2	2	1	1	2	2	2	1	2	2	2	3	430	0
4	2	4	5	0	2	0	0	1	0	2	1	0	1	2	0	0	0	0	2	1	0	1	1	461	2
5	1	3	5	2	1	0	1	2	1	2	0	0	2	2	0	2	2	1	2	0	0	1	4	457	2
3	2	4	5	0	2	1	2	1	0	0	1	0	0	2	0	2	1	0	0	0	0	2	3	469	2
4	1	2	3	1	0	2	2	0	1	2	0	1	1	0	0	2	0	1	0	0	1	1	3	473	4
2	2	4	3	1	0	1	0	0	1	0	1	1	2	0	1	2	0	1	0	1	1	1	3	478	3
3	1	3	5	0	2	1	2	2	1	2	2	2	2	2	1	2	1	1	2	2	2	3	3	562	3
2	1	3	2	2	2	0	0	2	2	0	2	0	2	2	0	1	2	2	0	2	0	1	4	733	1
3	1	2	3	1	0	1	2	2	0	1	1	0	2	2	1	2	2	0	0	1	0	1	4	705	4
3	2	5	5	1	1	2	2	2	0	1	2	2	2	1	1	2	2	0	1	2	2	2	3	781	2
3	1	3	5	1	1	2	1	2	2	2	2	2	1	1	1	1	1	2	2	2	2	1	3	2199	2
3	2	3	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	3	3	36	3
3	2	4	5	0	1	0	0	1	0	2	0	2	2	1	0	1	1	0	2	0	2	2	1	390	3
5	1	4	5	2	1	2	1	0	2	2	2	2	2	1	1	1	0	2	1	2	2	1	3	522	2
3	2	4	3	1	2	2	2	2	2	1	0	2	2	2	2	2	2	1	1	0	2	1	4	654	2
2	1	3	4	1	0	2	1	1	2	0	1	0	1	2	1	1	1	2	0	1	0	1	3	561	3
2	2	5	3	0	1	0	2	0	0	1	2	2	1	1	0	2	0	0	0	2	2	3	3	629	2
2	1	1	2	2	2	0	2	0	0	0	1	1	2	2	0	2	0	0	0	1	1	1	1	392	0
3	1	4	3	2	1	1	1	2	0	2	0	1	2	2	1	1	2	0	2	0	0	3	3	724	2
3	2	4	5	2	2	0	0	1	1	0	0	0	2	2	0	0	1	0	0	0	0	3	3	566	1
2	2	5	4	1	1	0	0	0	1	1	2	1	1	1	1	0	0	1	1	2	1	2	2	605	-1
5	1	1	2	0	1	2	1	2	2	1	0	2	0	0	2	1	2	2	0	0	2	2	2	1113	0
2	1	4	4	0	1	1	0	2	1	2	2	0	2	1	1	1	2	1	2	2	1	3	3	746	2
2	2	4	3	1	2	2	0	2	2	0	1	0	2	2	2	1	2	2	0	1	0	3	3	532	2
3	1	4	3	0	0	1	1	0	1	1	2	0	0	2	1	1	0	1	0	2	0	3	3	562	3
3	2	5	5	2	0	1	0	2	0	0	1	2	2	0	1	0	0	0	0	1	2	3	4	623	2
2	2	3	3	1	0	1	0	2	1	2	0	2	2	0	1	0	0	1	2	0	2	3	3	547	3
4	2	4	5	0	2	1	0	0	0	2	1	1	1	1	2	2	2	1	1	2	2	2	2	479	-3
3	1	3	3	2	0	0	0	0	1	0	2	2	2	2	0	1	0	1	0	2	2	3	3	831	3
3	2	4	2	2	0	0	0	1	1	0	0	0	2	0	0	1	1	0	0	0	0	1	3	672	2
2	2	5	1	2	2	0	0	1	1	0	0	2	2	2	0	1	1	0	0	0	2	2	3	608	2

2	1	3	3	0	2	0	0	2	1	1	2	1	0	2	0	1	2	1	1	1	1	1	1	443	2
3	1	4	2	0	0	2	0	1	2	1	2	0	0	2	2	0	1	1	1	2	0	2	3	455	3
3	1	5	5	2	2	2	2	2	1	1	1	1	2	2	2	2	2	1	1	0	1	1	3	578	1
2	1	3	4	1	0	1	1	1	1	1	1	0	1	0	1	1	1	0	1	1	0	1	1	459	1
2	1	4	3	1	2	1	2	0	2	2	0	2	1	2	1	2	0	2	1	0	2	3	3	466	1
2	2	4	4	2	0	2	0	2	2	1	0	0	2	0	2	1	2	1	1	0	0	3	3	520	2
3	2	3	3	0	2	0	0	0	0	1	1	0	1	2	0	1	0	0	1	1	0	1	3	503	2
3	1	2	1	1	0	1	1	2	0	0	0	1	1	2	0	1	2	0	0	0	1	1	5	977	3
3	1	3	5	1	1	2	2	2	0	0	2	0	1	1	1	2	2	0	0	1	0	2	4	587	2
3	2	3	3	0	2	0	2	2	2	1	0	0	0	2	0	2	2	2	0	0	0	1	3	715	1
2	1	3	3	2	0	2	0	0	0	2	0	1	2	0	2	1	0	0	2	0	0	2	3	715	2
3	1	3	4	1	1	1	0	1	2	1	2	2	1	1	1	1	1	1	1	1	1	1	1	76	4
4	1	4	4	2	2	1	2	1	2	1	2	2	2	2	1	2	2	1	1	1	1	1	1	136	2
2	1	3	2	1	0	2	0	1	0	2	0	1	0	2	0	1	0	2	0	1	0	1	1	63	5
3	1	4	5	2	2	1	1	0	0	1	2	0	2	2	1	2	1	0	1	2	1	1	1	92	-1
2	1	2	2	2	1	0	1	2	1	2	1	0	2	1	0	1	2	0	2	1	0	1	3	520	1
3	1	3	3	1	0	0	2	2	1	1	2	2	1	1	0	2	2	1	1	2	1	1	4	489	2
3	1	4	3	1	0	0	0	2	2	0	1	0	1	1	0	0	2	2	0	1	0	2	3	534	1
2	2	3	2	0	2	2	0	0	0	1	0	1	1	2	2	1	0	0	1	0	1	1	1	667	2
5	1	4	5	2	1	0	1	2	0	1	0	2	2	1	0	1	1	0	1	0	2	1	4	544	1
3	1	3	4	0	1	0	0	1	0	0	0	1	1	1	0	0	1	0	0	0	1	3	3	479	1
2	1	3	3	0	1	2	2	2	1	1	2	0	0	1	2	1	2	1	1	2	0	3	3	466	-1
2	1	3	1	1	1	0	1	1	2	0	1	1	1	1	0	1	1	1	0	1	1	1	1	439	1
3	1	5	2	0	1	2	1	0	0	1	0	1	1	1	2	1	0	0	0	0	1	3	3	570	2
4	1	2	5	1	1	0	0	0	0	2	0	2	1	0	0	0	0	0	2	0	2	1	3	479	-1
4	2	2	3	2	2	0	0	1	0	0	2	1	2	2	0	1	1	0	0	2	0	1	4	591	2
5	1	2	5	2	2	1	1	2	0	0	0	2	2	2	1	2	2	0	0	0	2	1	1	654	1
3	1	1	2	0	0	2	1	2	1	2	0	1	0	1	2	0	2	1	2	0	1	1	3	482	0
3	2	4	4	1	0	1	1	2	0	1	1	2	1	1	1	1	2	0	1	1	2	1	3	534	1
4	1	4	5	1	2	1	1	2	1	2	0	0	1	2	1	1	2	1	2	0	0	1	1	503	0
3	1	1	5	0	0	2	1	0	1	2	2	2	0	2	1	1	0	1	2	2	2	3	3	555	3
3	1	3	3	2	1	1	0	2	1	1	0	0	1	1	1	1	1	1	0	2	1	1	1	595	-1
5	1	1	3	1	0	1	1	1	1	2	1	2	1	1	1	0	1	1	2	1	2	3	3	535	0
4	1	1	4	0	1	1	1	2	0	1	2	2	2	1	0	2	2	0	1	2	2	1	4	683	4
3	2	5	5	0	0	0	2	0	0	0	0	2	1	1	0	2	0	0	0	0	2	4	4	814	2
2	1	5	4	1	2	2	2	0	2	0	2	0	1	2	2	2	0	2	0	2	0	3	3	529	0
3	1	5	5	0	2	2	0	2	1	0	0	0	1	2	2	1	2	1	0	0	0	4	4	517	2
4	1	4	1	1	2	2	0	2	0	2	2	2	1	2	2	0	2	0	2	2	2	1	1	568	0
4	1	2	1	2	0	0	1	2	0	1	2	2	2	0	0	2	2	0	1	2	2	1	1	422	1
3	2	4	3	1	2	1	1	1	1	0	1	1	2	2	1	2	1	1	0	1	1	3	3	479	2
3	1	5	4	2	1	2	0	0	1	2	2	2	2	2	2	1	0	1	2	2	2	3	3	515	2

2	1	1	2	2	2	1	1	2	2	1	0	1	2	2	1	1	2	1	1	0	1	1	1	597	1
3	1	3	2	1	0	1	2	1	0	0	1	0	1	2	1	2	1	0	0	1	0	1	1	566	2
4	1	4	4	1	1	1	1	1	2	2	0	1	1	2	1	2	1	2	2	0	1	1	1	558	2
5	1	2	3	1	2	1	1	0	0	0	2	0	1	2	1	2	0	0	0	2	0	3	3	460	1
3	2	3	2	2	1	1	2	2	1	1	0	2	2	1	1	2	1	1	1	0	2	1	1	538	1
5	1	1	2	2	2	1	0	0	2	1	0	2	2	2	1	1	0	2	1	0	2	1	3	682	1
4	1	5	3	1	0	0	0	1	1	1	1	2	1	1	0	0	1	0	1	1	2	1	3	556	2
3	1	4	4	1	1	1	1	0	0	2	0	2	1	0	1	1	0	0	2	0	2	1	1	500	-1
5	1	4	1	0	0	0	2	2	0	0	2	1	0	0	0	2	2	0	0	2	0	1	1	533	1
4	1	3	3	1	1	0	2	2	1	2	2	2	1	1	0	2	2	0	2	2	2	1	1	485	1
2	1	3	4	2	1	1	0	1	0	1	1	0	2	2	1	1	1	0	1	1	0	2	3	812	2
3	1	5	4	1	1	1	2	2	0	1	1	1	2	1	1	2	1	0	1	1	1	1	4	523	2
3	1	4	4	1	1	1	2	2	2	0	1	0	1	2	1	2	2	1	0	1	0	1	1	448	2
2	1	1	1	1	0	1	0	2	0	2	2	0	1	0	0	0	2	0	2	2	0	1	1	513	1
3	1	2	5	1	0	0	0	0	0	1	2	2	1	0	0	1	0	0	1	2	2	3	3	551	1
2	1	1	4	2	1	2	0	0	2	0	2	1	2	1	2	1	0	2	0	2	1	1	1	531	1
4	2	4	4	2	2	0	0	0	0	1	0	1	2	2	0	1	0	0	1	0	1	1	1	643	1
4	1	4	3	0	1	2	0	0	1	2	1	2	0	1	2	1	0	1	2	1	1	1	1	558	2
2	1	4	4	2	0	2	0	0	1	1	0	2	2	1	2	0	0	1	1	0	2	1	3	477	1
4	2	2	5	2	0	2	0	2	0	2	0	1	2	1	2	0	2	0	2	0	0	1	1	573	2
3	1	2	2	1	1	2	0	1	0	1	2	2	2	1	2	1	1	0	1	2	2	1	1	446	2
4	1	2	3	2	1	2	1	2	1	0	1	2	2	0	2	0	2	1	0	1	2	1	1	570	-2
5	1	2	1	1	0	0	0	1	2	1	0	0	1	0	0	2	1	2	1	0	0	1	1	524	2
3	2	1	2	1	0	2	2	0	2	2	2	2	2	1	2	2	0	2	2	2	2	3	3	518	2
2	1	2	4	0	0	1	0	1	2	0	2	1	0	0	1	1	1	1	0	2	1	1	1	622	2
4	1	3	5	0	0	2	1	2	0	0	2	0	1	1	2	1	2	0	0	2	0	1	3	455	2
5	1	2	5	2	0	1	0	1	2	1	0	2	2	1	1	1	1	2	1	0	2	1	1	541	2
5	1	2	2	1	2	1	0	1	2	1	2	1	2	2	1	0	1	2	1	2	1	1	1	460	1

Table 41: Game Data

A	g	t	e	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	b	e	t	s		
g	e	e	e	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	e	n	i	c		
e	n	d	h	1	2	3	4	5	6	7	8	9	1	2	2	3	4	5	6	7	8	9	j	m	o	
r	d	u	u	1	2	3	4	5	6	7	8	9	1	2	2	3	4	5	6	7	8	9	e	e	r	
4	1	3	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	4	2038	0	
4	1	3	3	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	699	-3
2	2	3	2	0	1	0	1	0	1	0	0	1	0	0	0	2	0	0	0	0	0	1	4	4	142	1

2	1	3	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	4	4	118	3
3	2	3	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	138	0
2	1	2	3	1	1	1	1	1	1	1	1	1	1	2	2	0	2	0	0	0	0	0	5	5	176	9
2	2	2	2	0	1	0	1	1	0	0	1	0	2	2	0	2	0	0	0	0	0	0	3	4	149	6
3	2	3	3	1	0	0	1	0	1	0	0	1	2	2	0	2	0	0	0	0	0	3	3	173	6	
2	2	3	3	0	1	0	0	2	0	1	0	0	2	2	1	1	0	0	0	0	0	4	4	891	6	
2	2	4	3	1	1	2	0	0	2	1	2	2	2	2	1	2	0	0	0	0	0	3	3	236	1 2	
2	1	3	3	1	1	2	1	2	2	1	2	1	2	2	0	2	0	0	0	0	0	3	3	233	1 3	
2	1	1	1	1	1	1	1	1	1	1	1	1	2	2	0	2	0	2	0	0	0	4	4	156	7	
2	1	4	4	1	1	2	0	0	2	1	0	0	2	2	0	2	0	0	0	0	0	4	4	142	9	
2	1	3	3	1	1	1	1	1	1	1	1	1	2	2	0	2	0	0	0	2	2	5	5	151	5	
2	2	4	3	0	0	0	0	0	2	1	0	1	2	2	0	2	0	0	0	0	0	4	3	259	1 0	
2	1	2	2	1	0	0	0	2	0	1	0	0	2	2	0	0	2	0	0	0	0	1	1	151	4	
2	2	3	2	1	1	1	1	1	1	1	1	1	0	1	0	0	0	1	2	0	1	1	1	417	0	
2	2	3	2	1	0	1	0	1	0	0	1	0	2	2	0	2	0	0	0	0	0	4	4	482	8	
2	1	1	1	1	1	1	1	0	0	0	0	0	2	2	0	0	0	0	0	0	0	1	1	143	2	
2	2	3	3	1	1	1	1	1	2	1	1	2	2	2	0	2	0	0	0	2	0	3	3	245	9	
2	1	3	2	1	1	2	1	2	2	1	2	2	2	2	0	2	0	0	0	0	0	4	4	218	1 4	
2	1	4	4	1	1	1	1	1	1	1	1	1	2	2	0	2	0	0	0	0	0	4	4	1071	9	
2	1	4	3	1	1	2	1	2	2	1	2	0	2	2	0	2	0	0	0	0	0	1	1	248	1 2	
2	2	3	2	1	1	1	1	1	1	1	1	1	2	2	0	2	0	0	0	0	0	3	3	405	9	
2	2	2	2	0	0	2	1	2	2	1	2	2	2	2	0	2	0	0	0	0	0	3	3	663	1 6	
2	1	2	1	1	1	1	1	1	1	1	1	1	2	2	0	2	2	0	2	0	0	1	1	141	5	
2	1	3	3	1	1	1	1	2	1	1	2	2	2	2	0	2	0	0	2	0	0	3	3	4368	1 0	
2	1	3	3	1	0	2	1	2	2	0	2	0	2	2	0	2	0	0	0	0	0	4	4	146	1 2	
2	1	2	2	0	0	2	1	2	2	1	2	0	2	2	0	2	0	2	2	0	2	3	3	238	8	
2	2	3	2	0	0	0	2	0	2	1	0	0	2	2	0	2	0	0	0	0	0	3	3	164	7	
2	1	2	2	0	0	2	1	2	2	0	2	2	2	2	0	2	0	0	0	0	0	4	4	450	1 5	
2	1	3	3	1	1	1	1	1	1	1	1	1	2	2	2	2	0	0	0	0	0	1	1	1173	7	
2	2	4	3	0	0	2	1	2	2	1	0	2	2	2	0	2	0	0	0	0	0	4	4	265	1 4	
2	2	2	2	1	1	1	1	2	2	1	2	2	2	2	0	2	0	0	0	0	0	3	3	1719	1 3	
2	2	3	2	0	1	2	0	2	2	0	2	2	2	2	0	2	1	1	0	1	1	3	3	324	1 1	
2	2	3	3	1	1	1	1	1	1	1	1	1	2	2	0	2	0	0	0	0	0	3	3	183	9	
2	1	1	2	1	1	1	1	1	1	1	1	1	2	2	0	0	2	0	0	0	0	1	1	181	5	
2	1	3	2	1	1	2	1	2	2	1	2	2	2	2	0	2	0	0	0	0	0	1	1	106	1 4	

2	1	3	3	0	0	2	0	2	2	0	2	2	2	2	2	0	0	0	0	0	3	3	108	1 4	
2	1	2	2	0	0	2	1	2	2	0	2	1	2	2	0	2	1	1	1	0	0	5	4	358	1 1
2	2	4	3	0	0	2	0	0	0	2	0	2	2	2	0	2	1	0	0	0	0	5	4	676	1 1
2	2	5	4	1	1	1	0	1	2	2	0	0	2	2	0	2	0	0	0	0	0	3	3	122	1 0
2	1	3	2	1	1	1	1	1	1	1	1	1	1	2	2	0	2	0	0	0	0	5	5	432	9
2	1	2	3	1	1	2	1	2	2	0	2	2	2	2	0	2	1	1	1	1	1	3	3	463	8
2	1	3	3	2	1	2	1	2	0	2	2	2	2	2	1	2	0	0	0	0	0	1	1	151	1 1
2	1	1	2	1	1	2	1	2	2	2	2	2	2	2	1	1	0	0	0	0	0	3	3	298	1 3
2	1	3	3	1	0	2	1	2	2	1	2	1	2	2	0	2	0	0	0	0	0	4	4	782	1 4
2	1	2	2	1	1	1	1	2	2	2	2	2	2	2	2	0	0	0	0	0	0	5	5	380	1 0
2	1	3	3	1	0	2	1	2	2	1	2	2	2	2	1	1	0	0	0	0	0	1	1	121	1 3
2	2	4	3	2	1	2	1	1	2	0	0	0	2	2	0	2	0	2	0	0	0	4	4	119	5
2	1	2	3	1	0	2	1	2	2	2	2	2	2	2	0	2	0	0	0	0	0	4	4	433	1 6
2	1	2	3	1	1	2	1	1	2	2	2	2	2	2	0	2	0	0	0	1	1	1	1	175	1 2
2	2	3	2	1	0	2	1	1	2	0	0	2	2	0	0	2	0	0	0	0	0	3	3	254	9
4	2	3	2	2	1	2	1	1	2	1	0	0	2	2	1	2	0	1	1	0	0	4	4	879	5
4	1	3	5	2	2	2	1	1	1	1	2	2	2	2	1	2	1	1	0	2	0	4	4	987	5
2	1	5	3	0	0	2	0	1	2	1	1	2	2	2	1	0	0	1	0	0	1	4	4	1073	1 0
2	1	2	3	1	0	2	1	1	2	2	2	2	2	2	1	2	0	0	1	1	1	4	4	1215	1 1
4	2	4	4	2	1	0	1	0	1	0	0	0	2	2	0	2	0	0	0	0	0	4	4	1058	3
4	2	4	3	1	1	2	1	2	1	0	2	2	2	2	1	2	1	0	0	0	0	4	3	740	1 0
2	1	4	3	2	2	2	2	2	2	2	2	2	2	2	0	2	0	0	0	1	1	4	3	713	1 0
3	2	4	3	0	0	0	2	1	2	1	2	1	2	1	0	2	0	1	0	1	0	4	4	752	8
2	1	3	2	1	1	2	1	2	2	1	2	2	2	2	1	2	0	1	0	0	0	1	1	644	1 2
2	1	3	3	1	0	2	1	1	1	0	2	1	2	1	0	2	0	0	0	1	1	5	4	695	8
2	1	2	2	0	0	2	0	1	2	0	2	1	0	0	2	0	1	2	0	2	1	1	1	191	0
2	2	4	3	1	0	1	1	1	2	1	2	2	2	2	2	0	1	1	1	1	1	3	3	1091	7
5	2	3	4	0	1	2	1	0	2	1	0	1	1	2	1	0	0	1	0	0	0	4	4	667	5
2	2	5	3	0	0	2	1	0	0	2	0	2	2	2	1	2	0	0	2	0	1	5	4	707	7
4	1	3	3	0	0	0	1	1	2	2	0	0	1	2	0	2	1	1	1	0	0	4	3	1054	6
4	1	4	4	2	1	1	2	2	0	2	2	0	2	2	0	2	1	0	2	1	0	4	4	727	4
3	1	3	3	1	1	2	2	0	0	0	2	1	0	0	1	2	0	0	0	1	1	4	4	827	0
2	1	2	2	1	1	2	2	2	2	0	2	0	2	2	1	2	1	1	0	1	0	5	5	803	6
5	1	1	1	0	0	0	0	0	2	1	1	2	2	2	0	1	0	1	1	1	1	4	3	619	7

2	1	2	2	2	1	1	2	0	0	1	1	1	2	2	0	2	0	0	0	1	1	4	4	680	3
4	2	4	4	2	1	2	1	1	0	2	0	1	2	1	2	1	1	0	2	0	1	3	3	574	0
4	1	3	3	0	2	2	2	1	2	2	2	2	1	2	1	2	0	1	2	1	1	4	4	739	6
3	1	3	2	1	1	0	1	0	1	2	1	2	2	2	0	2	0	1	1	1	1	4	3	905	5
3	1	3	4	2	0	0	0	0	0	2	1	0	2	2	0	1	0	0	1	0	0	3	3	652	5
2	1	3	3	2	0	2	2	0	1	1	0	0	2	1	1	2	0	1	0	0	0	3	3	787	3
3	2	4	4	1	0	0	2	1	2	2	2	2	2	1	0	2	1	0	1	1	0	4	4	1148	8
2	1	1	2	1	2	0	2	2	2	2	2	1	2	2	0	2	1	1	1	1	1	4	4	1075	5
5	1	4	5	2	0	2	1	1	0	0	2	0	2	0	2	1	1	0	0	2	0	4	4	1108	0
2	2	4	4	0	0	1	2	1	1	0	0	2	0	0	1	2	1	1	0	0	2	1	1	1158	0
2	1	2	2	0	1	2	2	1	2	2	2	0	0	1	2	2	1	2	2	2	0	4	4	983	0
3	1	3	2	0	2	0	2	0	0	2	0	0	2	0	0	2	0	0	0	0	0	5	4	2012	2
2	1	2	2	1	2	1	1	1	2	1	2	1	2	2	0	2	0	1	0	1	0	5	5	1203	8
3	1	3	5	2	2	0	2	0	0	2	1	0	2	2	0	2	0	0	1	0	0	5	3	1203	2
2	2	2	2	0	2	0	0	0	0	2	2	1	2	2	0	1	0	0	0	1	0	5	5	1204	7
2	2	2	1	1	2	2	0	2	1	1	2	1	1	2	2	0	2	1	1	2	1	5	5	1241	0
3	1	2	3	2	1	1	0	0	1	1	2	2	2	2	0	1	0	0	1	1	1	5	5	1039	6
2	2	4	4	0	2	2	0	0	2	1	2	2	2	2	0	1	0	0	0	1	1	5	5	1155	1 0
2	1	2	2	0	2	2	2	0	2	2	0	2	2	2	1	2	0	1	1	0	1	5	5	1109	6
2	2	4	3	1	0	0	2	0	0	0	1	1	2	1	0	2	0	0	2	1	0	5	5	954	1
2	1	2	2	1	1	1	1	0	0	2	1	0	2	2	0	1	0	0	0	0	0	4	4	1020	6
2	1	2	2	0	1	1	1	1	2	1	1	2	2	2	1	2	1	1	0	0	1	4	4	1072	8
4	2	4	4	2	0	1	0	1	2	1	0	2	2	2	0	2	1	1	0	0	1	4	4	1005	8
4	1	2	2	1	2	0	0	0	2	2	2	1	2	2	0	2	0	1	0	1	0	5	5	1687	8
3	2	4	3	2	1	1	1	0	2	1	2	0	2	0	2	1	0	0	0	2	1	5	4	1413	0
2	2	4	4	2	1	1	0	0	2	2	2	0	2	2	0	2	0	0	0	0	0	5	5	1038	1 0
4	2	2	3	2	0	0	1	0	0	2	0	2	2	2	0	2	0	0	0	0	1	4	4	1009	6
2	2	3	4	1	0	0	1	0	2	0	0	0	2	2	0	2	0	1	1	0	0	5	5	1187	4
4	1	3	3	0	2	1	2	2	1	0	2	0	2	2	0	1	0	0	0	1	0	5	5	1073	6
2	1	2	3	0	0	1	0	2	0	2	0	2	2	2	0	1	1	0	1	0	1	4	4	1101	9
2	1	2	2	1	2	1	1	2	1	0	2	1	2	2	0	2	1	0	0	1	2	5	5	1394	5
5	1	4	5	0	2	0	1	1	2	1	2	0	2	2	0	2	0	1	0	1	0	5	5	1224	7
3	1	4	2	0	2	1	0	2	1	0	1	1	2	2	1	2	1	0	0	0	0	5	5	1388	8
2	2	2	1	1	2	0	2	1	0	2	2	0	2	2	0	2	0	0	0	1	0	5	5	1032	5
3	2	3	3	0	0	0	2	2	0	0	1	1	2	2	0	2	1	0	0	0	0	5	5	1756	7
3	1	4	3	0	0	0	0	0	0	1	0	1	2	2	0	2	0	0	0	0	0	5	5	1653	8
2	2	5	3	0	1	0	2	0	1	0	0	2	2	2	0	2	0	0	0	0	1	5	4	1147	5
3	1	4	3	0	1	2	2	2	2	1	1	0	2	2	1	2	1	0	0	0	0	4	4	1279	9
3	1	4	4	2	2	0	0	0	2	0	0	2	2	2	0	2	0	1	0	0	1	5	5	658	4
5	1	2	4	2	1	1	2	1	2	0	2	0	2	2	0	2	0	1	0	0	0	5	5	1090	6

4	1	3	3	1	1	0	1	1	0	0	2	2	2	2	0	2	0	0	1	0	1	5	5	1219	6
3	1	4	3	0	0	2	2	2	1	2	0	2	2	2	1	2	1	0	1	0	1	5	5	1674	9
4	1	3	3	2	0	0	2	2	2	0	1	1	2	1	0	2	1	0	0	0	0	4	4	1045	6
3	1	3	2	1	0	1	1	0	0	2	1	1	2	2	0	2	0	0	0	0	1	5	5	1318	8
4	1	3	4	0	2	2	2	2	0	2	1	1	2	2	1	2	1	0	1	0	0	5	5	1293	7
2	1	3	3	2	1	0	1	1	2	0	1	0	2	2	0	2	0	1	0	1	0	5	4	1199	4
2	1	4	5	2	2	0	2	2	0	1	2	2	2	2	0	2	0	0	0	0	0	5	5	1104	7
3	2	3	5	1	2	2	1	0	2	1	0	1	2	2	0	2	0	0	0	0	0	5	5	1185	8
3	2	5	5	1	0	1	2	1	1	0	0	0	2	2	0	2	0	0	0	0	0	5	5	959	6
3	1	4	4	2	0	1	1	2	2	2	2	0	2	2	0	2	1	1	0	0	0	5	5	930	1 0
3	1	4	5	2	2	1	1	1	2	2	2	1	2	2	0	2	0	0	0	0	0	5	5	1403	1 0
2	1	2	2	0	0	2	0	0	0	2	0	1	2	2	2	1	0	0	1	0	0	5	5	886	7
3	2	3	3	1	2	1	0	2	1	0	1	2	2	2	0	2	1	0	0	0	1	5	5	1339	8
3	2	4	5	1	0	1	1	0	0	1	1	1	2	1	0	2	0	0	1	0	0	5	5	779	6
4	1	3	5	1	2	1	2	1	2	2	0	2	2	2	0	2	1	1	1	0	1	5	5	931	5
3	2	4	4	0	1	0	1	1	1	2	0	2	2	2	0	2	0	0	1	0	1	5	5	971	8
3	1	2	5	0	1	0	0	2	1	2	1	2	2	2	0	1	1	0	0	0	1	5	5	940	1 0
4	1	3	5	2	0	1	0	2	1	2	0	1	2	2	0	2	1	0	0	0	0	5	5	886	1 0
3	1	4	5	2	1	2	0	1	2	0	1	1	2	2	1	2	0	1	0	0	0	5	5	833	8
3	1	4	5	1	0	0	0	2	0	2	1	1	2	2	0	2	1	0	1	0	0	5	5	908	9
5	2	3	5	1	2	0	1	0	0	2	2	1	2	2	0	2	0	0	1	1	1	5	5	1137	4
2	1	4	3	2	1	2	2	2	1	0	0	2	2	2	1	2	1	0	0	0	0	5	5	1054	6
3	1	4	5	1	1	0	0	1	0	2	1	2	2	2	0	1	1	0	1	1	1	5	5	900	5
3	1	3	3	0	1	2	1	1	2	0	0	2	2	2	1	2	0	1	0	0	1	5	5	1213	8
3	2	4	3	1	1	1	1	1	2	1	2	1	2	2	0	2	0	1	1	1	0	5	5	1308	8
3	2	3	3	0	2	0	0	2	0	2	0	1	2	2	0	2	0	0	1	0	0	5	5	1228	8
3	1	3	4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	40	0
3	1	3	2	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	3	3	124	- 3
4	1	3	4	1	2	2	2	2	2	1	0	2	2	2	1	2	1	1	0	0	0	5	5	1504	7
4	2	4	5	1	0	0	1	1	2	0	1	1	2	1	0	2	0	1	0	0	0	5	5	1369	7
4	1	4	5	2	1	0	1	0	2	2	0	2	2	2	0	2	0	1	0	0	1	5	5	1484	6
5	1	3	5	0	1	2	2	2	1	2	0	2	2	2	1	2	1	0	1	0	1	4	4	813	8
2	2	4	3	0	0	0	1	2	2	2	0	0	2	2	0	2	1	0	0	0	0	5	5	1808	1 0
4	1	4	3	2	2	0	2	1	0	2	2	1	2	2	0	2	0	0	1	1	0	5	5	1845	4
3	1	3	5	2	2	1	0	1	2	1	2	2	2	2	0	2	1	0	0	1	1	4	4	1169	8
3	1	3	3	2	1	1	0	2	1	1	2	2	2	2	1	1	1	1	0	1	2	5	5	1202	5
4	2	4	5	2	1	2	0	2	0	1	0	1	2	2	1	2	0	0	0	0	0	4	4	757	8
2	1	2	2	2	0	0	1	2	0	1	0	2	2	2	0	2	1	0	0	0	1	5	5	1464	6
2	1	4	4	1	2	0	2	1	1	0	2	2	2	2	0	2	0	0	0	1	1	5	5	2132	5

2	1	3	3	0	1	0	0	1	0	2	2	1	2	2	0	1	1	0	0	0	1	4	4	861	8
3	1	3	3	1	2	1	1	1	2	2	1	0	2	2	0	2	0	1	1	0	0	5	5	920	7
2	2	5	2	1	1	2	0	0	2	0	2	0	2	2	1	2	0	1	0	1	0	5	5	1367	7
3	1	3	2	1	1	0	2	1	1	1	1	1	2	2	0	2	0	0	0	0	0	5	5	1380	7
3	1	4	4	2	2	0	0	2	0	1	2	2	2	2	0	1	1	0	0	1	1	4	5	1106	5
4	1	2	4	0	0	2	2	1	0	2	1	0	1	2	1	2	1	0	1	0	0	5	5	836	6
3	2	4	3	0	2	1	2	0	0	2	2	1	2	2	0	2	0	0	0	1	0	5	5	1479	7
2	1	2	5	0	0	1	2	0	2	2	0	0	2	2	1	2	0	1	1	0	0	5	5	1069	6
3	2	4	5	2	1	0	2	1	1	1	0	2	2	2	0	2	0	0	0	0	0	5	5	1280	6
2	1	2	1	2	2	1	2	0	2	1	1	0	2	2	0	2	0	1	0	0	0	5	5	1511	4
3	1	2	2	2	1	1	0	2	1	1	2	0	2	2	0	2	1	0	0	0	0	5	5	1406	9
3	1	3	5	1	1	0	2	1	0	0	1	2	2	2	0	2	0	0	0	0	1	5	5	1475	5
3	1	3	3	0	1	2	0	1	2	2	1	1	2	2	2	1	0	1	0	0	0	5	5	1578	10
3	1	3	3	0	0	1	2	2	0	2	2	2	2	2	0	2	1	0	0	1	1	5	5	1121	10
3	2	5	4	1	2	2	2	0	0	1	0	0	2	2	0	2	0	0	0	0	0	5	5	1085	4
3	1	4	5	2	1	1	1	0	1	2	2	1	2	2	0	2	0	1	1	0	0	5	5	1016	7
3	1	3	3	1	0	0	1	1	0	1	2	0	2	1	0	2	1	0	0	1	0	5	5	1256	5
2	2	5	3	2	0	0	0	0	1	1	0	2	2	2	0	2	0	0	0	0	1	5	5	1368	7
3	1	4	5	2	2	0	0	2	2	1	2	1	2	2	0	1	1	2	0	2	0	5	5	999	4
2	0	3	3	2	2	0	0	1	1	0	0	2	2	2	0	1	0	0	0	0	1	4	4	247	4
3	1	3	3	1	1	2	1	2	2	1	2	1	2	2	1	2	0	0	0	0	1	4	4	451	11
2	1	1	1	0	1	1	0	2	1	1	0	2	1	1	0	2	2	0	0	0	0	5	5	1906	8
2	1	2	2	2	0	1	2	1	1	2	1	0	2	2	0	1	0	0	0	0	0	5	5	1804	7
3	1	3	3	1	0	1	1	0	0	1	1	1	2	2	0	2	0	0	0	0	0	5	5	1430	8
5	1	5	5	2	1	2	0	0	0	2	1	2	2	2	0	1	0	0	1	0	0	5	5	1740	8
3	0	4	1	2	1	2	2	2	1	2	2	2	2	2	0	2	1	0	0	0	1	5	5	1641	10
3	1	4	5	2	0	2	0	1	1	2	2	1	2	2	0	0	0	0	1	0	0	5	5	1779	10
4	0	5	4	1	0	0	1	0	1	1	1	1	2	1	0	2	0	0	0	0	0	5	5	1205	7
5	0	2	3	1	2	2	2	2	2	2	2	2	2	2	1	2	0	0	1	0	0	5	5	1381	11
4	1	2	2	2	1	0	0	2	2	0	2	2	2	2	0	1	1	0	0	0	1	5	5	1305	8
5	1	2	5	2	2	1	1	2	0	0	0	2	2	2	0	0	1	0	0	0	1	5	5	1688	2
2	0	4	1	2	1	1	0	2	1	1	1	0	2	2	0	1	1	0	0	0	0	5	5	1218	7
4	1	2	2	0	0	0	1	1	1	1	2	2	2	2	0	2	0	0	0	1	1	5	5	1586	10
3	1	5	1	0	2	1	1	0	2	0	0	2	1	2	0	2	0	1	0	0	1	5	5	1055	5
3	1	3	4	0	0	1	2	1	1	2	2	1	2	2	0	1	0	0	1	1	0	5	5	1096	9
4	0	3	1	2	2	1	0	2	2	2	2	0	2	2	1	1	1	1	2	1	0	1	1	1796	4
2	0	2	2	0	2	1	2	0	1	0	2	0	2	2	0	2	0	0	0	1	0	5	5	1618	5
3	1	4	3	0	1	1	2	1	2	1	2	2	0	1	1	2	1	2	1	2	2	5	5	1245	0

4	0	5	5	2	0	1	0	1	1	0	1	0	2	1	0	2	0	0	0	0	0	5	4	1344	7
2	1	5	1	1	1	1	2	0	1	0	0	1	2	2	0	2	0	0	0	0	0	5	5	1519	5
3	0	2	1	0	0	0	2	0	0	0	2	2	1	1	0	2	0	0	0	1	1	4	5	1527	4
4	0	4	5	0	2	2	1	2	1	2	2	2	0	2	2	1	2	1	2	2	2	5	5	1451	0
2	1	2	1	2	0	0	0	2	0	2	1	1	2	2	0	1	1	0	1	0	0	5	5	1074	7
4	1	2	1	1	1	0	1	0	2	0	2	0	2	2	0	2	0	1	0	1	0	5	5	1290	5
3	1	2	2	2	1	2	2	0	0	0	0	1	2	2	1	2	0	0	0	0	0	5	5	1538	3
3	1	2	1	1	1	1	0	0	2	0	2	0	2	2	0	1	0	1	0	1	0	5	5	1032	6
2	1	3	5	0	2	0	1	2	1	1	0	1	1	2	0	2	1	0	2	0	0	1	1	1084	4
4	0	1	2	2	0	2	2	1	1	2	1	1	2	1	1	2	0	0	1	0	0	5	5	1621	7
3	1	3	3	2	1	2	2	1	0	2	1	1	2	2	1	2	0	0	1	0	0	5	5	1559	6
5	1	5	5	0	0	1	2	1	2	1	0	2	0	0	1	2	1	2	1	0	2	5	5	2085	0
5	1	4	4	1	2	1	1	2	2	2	1	1	2	2	0	1	1	0	1	0	0	5	5	1127	8
3	1	3	4	2	0	1	2	2	1	0	2	1	2	2	1	2	0	0	0	1	0	5	5	1157	7
3	1	5	3	0	1	1	1	1	0	1	1	1	2	2	0	2	0	0	0	0	0	5	5	2000	9
3	1	4	2	0	0	0	0	1	0	1	2	0	2	2	0	2	1	0	2	1	0	5	5	1114	6
2	0	5	4	0	0	2	0	2	0	0	2	0	2	2	1	2	1	0	0	1	0	5	5	1159	9
4	1	3	1	0	0	2	2	2	2	2	2	2	1	2	1	2	1	1	0	1	1	5	5	1102	1 0
5	1	5	5	0	1	1	2	0	1	1	1	1	2	2	0	2	0	0	0	0	0	5	5	1555	8
2	1	5	5	0	2	0	2	0	1	2	0	0	2	2	0	2	0	1	1	0	0	5	5	1288	3
3	1	2	4	2	0	2	1	1	1	0	2	0	2	2	1	2	1	1	0	1	0	5	5	1191	5
2	1	2	2	0	2	1	0	0	0	2	0	1	1	2	0	2	0	0	1	0	1	5	5	1502	5
2	1	3	2	0	2	1	1	2	2	2	0	2	1	2	0	2	1	1	1	0	2	5	4	1435	6
3	1	5	5	1	2	1	2	1	2	1	1	2	2	2	0	2	0	1	0	0	1	5	5	1281	7
4	1	5	2	0	1	2	2	2	1	2	2	1	2	2	1	2	0	0	1	1	0	5	5	1243	1 0
2	1	3	4	1	2	2	2	2	1	1	2	2	2	2	0	2	1	0	0	1	1	1	1	933	8
5	0	3	4	2	0	0	0	2	1	2	2	2	2	2	0	1	1	0	0	0	1	5	5	1438	1 0
3	1	1	1	1	0	2	0	0	1	2	2	0	2	2	1	2	0	0	1	0	0	5	5	1323	1 0
2	1	1	4	2	0	2	0	2	0	0	1	1	2	2	1	2	1	0	0	0	0	5	5	1363	8
4	0	5	1	0	1	2	0	0	0	0	2	1	2	2	1	1	0	0	0	0	0	1	1	1222	8
2	1	2	3	1	1	0	1	0	0	1	0	0	2	2	0	2	0	0	0	0	0	5	5	1495	4