

5-13-2006

## Cyber-Crime Fear and Victimization: An Analysis of a National Survey

Abdullah Al-Shalan

Follow this and additional works at: <https://scholarsjunction.msstate.edu/td>

---

### Recommended Citation

Al-Shalan, Abdullah, "Cyber-Crime Fear and Victimization: An Analysis of a National Survey" (2006).  
*Theses and Dissertations*. 1244.  
<https://scholarsjunction.msstate.edu/td/1244>

This Dissertation - Open Access is brought to you for free and open access by the Theses and Dissertations at Scholars Junction. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of Scholars Junction. For more information, please contact [scholcomm@msstate.libanswers.com](mailto:scholcomm@msstate.libanswers.com).

CYBER-CRIME FEAR AND VICTIMIZATION:  
AN ANALYSIS OF A NATIONAL SURVEY

by

Abdullah Alshalan

A Dissertation  
Submitted to the Faculty of  
Mississippi State University  
in Partial Fulfillment of the Requirements  
for the Degree of Doctor of Philosophy  
in Sociology  
in Department of Sociology, Anthropology, and Social Work

Mississippi State University

May 2006

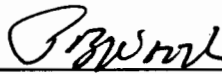
Copyright by  
Abdullah Alshalan  
2006

CYBER-CRIME FEAR AND VICTIMIZATION:  
AN ANALYSIS OF A NATIONAL SURVEY

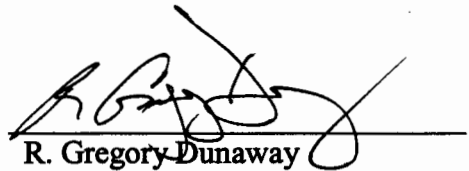
By

Abdullah Alshalan

Approved:



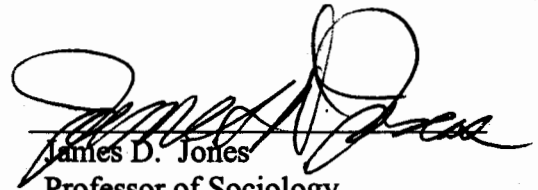
Peter B. Wood  
Professor of Sociology  
(Director of Dissertation)



R. Gregory Dunaway  
Professor of Sociology  
(Committee Member)



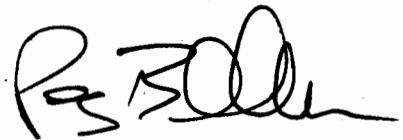
Xiaohe Xu  
Professor of Sociology  
(Committee Member)  
(Graduate Coordinator)



James D. Jones  
Professor of Sociology  
(Committee Member)



Kent R. Kerley  
Assistant Professor of Sociology  
(Committee Member)



Phillip B. Oldham  
Dean of the College of Arts and  
Sciences

Name: Abdullah Alshalan

Date of Degree: May 13, 2006

Institution: Mississippi State University

Major Field: Sociology

Major Professor: Dr. Peter B. Wood

Title of Study: CYBER-CRIME FEAR AND VICTIMIZATION: AN ANALYSIS  
OF A NATIONAL SURVEY

Page in Study: 204

Candidate for Degree of Doctor of Philosophy

The aim of this study was to investigate cyber-crime victimization among Internet users in the United States by: 1) assessing the factors that impact computer virus victimization; 2) assessing the factors that impact cyber-crime victimization; and 3) predicting fear of cyber-crime. Two domains in criminology were applied to the study of cyber-crime phenomenon: routine activity theory, and the fear of crime literature. Three independent models were developed to predict computer virus victimization, cyber-crime victimization, and fear of cyber-crime. Measures of routine activity theory applied to cyber-crime victimization include risk exposure, and suitable targets were created. A more reliable measure of fear of cyber-crime and a measure of perceived seriousness of cyber-crime were created. The 2004 National Cyber Crime Victimization Survey dataset was used in this project. Logistic Regression and OLS Regression were utilized to predict computer virus victimization, cyber-crime victimization, and fear of cyber-crime.

The findings of this study indicate that routine activity theory was a powerful predictor of computer virus victimization and cyber-crime victimization. That is, risk exposure and suitable targets helped determine the victimization. The study also found that cyber-crime victimization, gender, and perceived seriousness were predictive of fear of cyber-crime. Discussion of the findings and theoretical and policy implications were offered.

## DEDICATION

This dissertation is dedicated to the memory of my late father, Ahmed. May Allah bless him and rest him in Paradise. To my mother, Haya. May Allah reward and grant her with a good health. To my beloved and sweetheart wife, Nourah. To my sunshine children, Ahmed and Sadeem.

## ACKNOWLEDGEMENTS

Thanks and praises are all to be to Allah, who bestowed me with all bounties, and helped to complete this project. I am most grateful to all of those who have made this project possible. First and foremost, I acknowledge my major advisor, Dr. Peter Wood, who guided me and shared with me his rich knowledge to complete this dissertation. His knowledge and guidance were the lights that shed on my way toward the end of this project. I am so thankful to him for giving me the chance to be the first to work on the 2004 National Cyber Crime Victimization Survey dataset.

My gratefulness extends to all of my committee members, Dr. Gregory Dunaway, Dr. Xiaohe Xu, Dr. James Jones, and Dr. Kent Kerley for their sincere help and efforts they put in this dissertation. Thanks to Dr. Gregory Dunaway for helping me to extend the scope of this dissertation. Thanks to Dr. Xiaohe Xu for his generous help in teaching me the statistics, which had a great effect on the development of this dissertation. My thanks extend to Dr. James Jones for the valuable comments he made for this dissertation. Also, my thanks go to Dr. Kent Kerley for his effort in developing this project.

My sincere and undeniable gratefulness go to my beloved and sweetheart wife, Nourah, for her endless emotional support throughout the most challenging venture of my life. She has scarified her time, and put great efforts to provide me with a healthy place where I could study and finish my dissertation. Without her loving support I would not be



able to finish. I am so grateful to my children, Ahmed and Sadeem, who have brought joy to my life

I am most thankful to my mother for her love, prayers, and support, and to my brothers Dr. Fahad, Mohammed, and Abdulrahman for their support and encouragement. My thanks and appreciations go to my friend Dr. Paulette Meikle-Yaw for her endless support throughout my studies. Also, I would like to thank my friend Christy Flatt for her help editing my dissertation.

## TABLE OF CONTENTS

	Page
DEDICATION .....	ii
ACKNOWLEDGEMENTS .....	iii
LIST OF TABLES .....	viii
LIST OF FIGURES .....	xi
CHAPTER	
I. INTRODUCTION .....	1
The Objectives of the Study .....	4
The Significance of the Study .....	5
II. REVIEW OF THE LITERATURE .....	9
Cyber-Crime .....	9
How Cyber-Crime Happens .....	13
Cyber-Crime Victimization .....	18
Is Cyber-Crime a White-Collar Crime? .....	20
Routine Activity Theory .....	24
Fear of Crime .....	33
Cyber-Crime Victimization and Fear of Cyber-Crime .....	41
Hypotheses .....	43
III. METHODOLOGY .....	45
Data .....	45
Operational Measurement .....	46
Computer Virus Victimization .....	47
Cyber-Crime Victimization .....	47
Fear of Cyber-Crime .....	48
Frequency .....	49
Duration .....	50
Id-target and Money-target .....	50
Knowing Victim .....	52
Having Children with Access to the Internet .....	52

CHAPTER	Page
Perceived Seriousness.....	53
Gender.....	54
Race.....	54
Age.....	54
Education.....	55
Income.....	55
Rural-Urban Place of Residence.....	56
Interaction Terms.....	57
Age*Gender.....	57
Gender*Cyber-Crime Victimization.....	58
Plan of Analysis.....	58
Study Limitation.....	64
<b>IV. UNIVARIATE AND BIVARIATE STATISTICS.....</b>	<b>66</b>
Univariate Statistics.....	66
Factor Analysis.....	72
Bivariate Statistics.....	74
Cyber-Crime Victimization.....	74
Fear of Cyber-Crime.....	82
Internet Behavior.....	85
Correlation Matrix.....	89
<b>V. MULTIVARIATE ANALYSIS.....</b>	<b>93</b>
Logistic Regression Diagnoses.....	95
Computer Virus Victimization Models.....	96
Model 1.....	96
Model 2.....	97
Model 3.....	98
Cyber-Crime Victimization Models.....	103
Model 1.....	103
Model 2.....	104
Model 3.....	105
Model 4.....	106
Fear of Cyber-Crime Models.....	111
OLS Regression Diagnosis.....	111
Model 1.....	111
Model 2.....	112

CHAPTER	Page
Model 3 .....	115
Model 4 .....	116
Summary of The Major Findings.....	119
Computer Virus Victimization Models.....	119
Cyber-Crime Victimization Models .....	119
Fear of Cyber-Crime Models .....	120
VI. DISCUSSION AND CONCLUSION.....	122
Computer Virus Victimization.....	125
Cyber-Crime Victimization .....	130
Fear of Cyber-Crime .....	137
Conclusion .....	145
Theoretical and Policy Implications .....	148
Future Research .....	152
BIBLIOGRAPHY.....	158
APPENDIX A.....	164
APPENDIX B.....	194
APPENDIX C.....	198

## LIST OF TABLES

TABLE		Page
1	The Matrix of Cyber-Crime: Level of Opportunity by Type of Crime .....	10
2	Routine Activity & Cyber-Crime Victimization .....	31
3	Taxonomy of Crime Perception .....	34
4.1	Frequencies and Percentages of Selected Variables.....	67
4.2	Descriptive Statistics of Selected Variables .....	68
4.3	Frequencies and Percentages of Cyber-Crime Victimization .....	70
4.4	Frequencies and Means of Fear of Cyber-Crime .....	71
4.5	Factor Analyses of Fear of Cyber-Crime Items .....	73
4.6.1	Cross-Tabulation of Cyber-Crime Victimization by Selected Variables ..	76
4.6.2	Mean Comparisons of Selected Variables.....	78
4.6.3	Mean Comparisons of Selected Variables.....	79
4.6.4	Mean Comparisons of Selected Variables.....	79
4.6.5	Mean Comparisons of Selected Variables.....	80
4.6.6	Mean Comparisons of Selected Variables.....	81
4.6.7	Mean Comparisons of Selected Variables.....	81
4.6.8	Mean Comparisons of Selected Variables.....	82
4.7	Mean Comparisons of Fear of Cyber-Crime Items by Gender .....	83

TABLE	Page
4.8 Mean Comparisons of Fear of Cyber-Crime Items by Race .....	84
4.9 Mean Comparisons of Fear of Cyber-Crime Items by Type of Residence .....	85
4.10 Cross-tabulation of Internet Activities by Gender.....	86
4.11 Cross-tabulation of Internet Activities by Race .....	87
4.12 Mean Comparisons of Selected Variables by Gender.....	88
4.13 Mean Comparisons of Selected Variables by Race.....	88
4.14 Mean Comparisons of Selected Variables by Type of Residence.....	89
4.15 Correlation Matrix of All Variables .....	91
5.1 Logistic Regression of Computer Virus Victimization (Dependent Variable: 1 =Yes).....	101
5.2 Logistic Regression of Cyber-Crime Victimization (Computer Virus and Other Types of Cyber-Crime) (Dependent Variable: 1 =Yes) .....	109
5.3 OLS Regression of Fear of Cyber-Crime.....	114
5.4 OLS Regression of Fear of Cyber-Crime (Interaction Terms).....	118
6.1 Hypotheses and Support of Findings.....	123
6.2 Logistic Regression of Computer Virus Victimization .....	129
6.3 Logistic Regression of Cyber-Crime Victimization.....	137
6.4 OLS Regression of Fear of Cyber-Crime.....	145
B.1 Cross-Tabulation of Cyber-Crime Victimization by Selected Variables..	195
C.1 Logistic Regression of Computer Virus Victimization (Interaction Terms) (Dependent Variable: 1 =Yes) .....	199

TABLE		Page
C.2	Logistic Regression of Computer Virus Victimization (Interaction Terms) (Dependent Variable: 1 =Yes) .....	200
C.3	Logistic Regression of Computer Virus Victimization (Interaction Terms) (Dependent Variable: 1 =Yes) .....	201
C.4	Logistic Regression of Cyber-Crime Victimization (Interaction Terms)(Dependent Variable: 1 =Yes) .....	202
C.5	Logistic Regression of Cyber-Crime Victimization (Interaction Terms)(Dependent Variable: 1 =Yes) .....	203
C.6	Logistic Regression of Cyber-Crime Victimization (Interaction Terms)(Dependent Variable: 1 =Yes) .....	204

## LIST OF FIGURES

FIGURE		Page
1	Cyber-Crime and White-Collar Crime Shared Characteristics .....	24
2	Cyber-Crime Setting. Adapted from Felson, Marcus.(2002) Crime and Everyday Life .....	33
3	Computer Virus Victimization Model.....	62
4	Cyber-Crime Victimization Model.....	62
5	Fear of Cyber-Crime Model .....	63
6.a	The Consequences of Fear of Cyber-Crime .....	155
6.b	The Consequences of Fear of Cyber-Crime .....	156
6.c	The Consequences of Fear of Cyber-Crime .....	157



## CHAPTER I

### INTRODUCTION

The 21<sup>st</sup> century is signified by the information age. Over the last few years the Internet has expanded exponentially. Currently, about 820 million people use the Internet, an increase of 126 percent from 2000 to 2005 (InternetWorldStats.com, 2005). Given the relative ease of using the Internet, and increasingly more affordable access to personal computers with high-speed modems, people can communicate, form new friendships, shop, entertain, learn, do business, and pay bills online. The World Wide Web creates what is called the virtual world or cyberspace, which is defined as an “indefinite place where individuals transact and communicate” (Britz, 2004 P 2). Cyberspace is characterized as a place where no physical or social boundaries deprive people from living in it.

Unfortunately, cyber space generates a new type of crime called Cyber-Crime by creating new opportunities for criminals (Wall, 2005). Criminals can surf cyberspace and commit crimes such as hacking, fraud, computer sabotage, drug trafficking, dealing in child pornography, and cyberstalking (United Nations Crime and Justice Information Network UNCJIN, 1999) without being caught or detected.

According to the Bureau of Justice Statistics (BJS) the nation's violent crime rate fell 10 percent in 2001 continued decline since 1994. Violent victimization and property crime rates in 2001 are the lowest recorded since the National Crime

Victimization Survey's inception in 1973. For instance, the personal theft rate fell 33%; and the property crime rate fell 6%, from 178 to 167 victimizations per 1,000 households from 2000 to 2001 (BJS, 2002).

On the other hand, the number of victims of Cyber-Crime is on rise, given the increase in the number of Internet users. In 2004, the Internet Crime Complaint Center (IC3) referred 190,143 complaints to enforcement agencies on behalf of individuals. These complaints included many different types of fraud such as auction fraud, non-delivery, and credit/debit card fraud, as well as non-fraudulent complaints, such as computer intrusions, spam/unsolicited e-mail, and child pornography. This is almost a 100 percent increase over 2003 when 95,064 complaints were referred. The total dollar loss from all referred cases of fraud was \$68.14 million with a median dollar loss of \$219.56 per complaint.

The increasing number of victims of Cyber-Crimes who suffer financial loss, or who are threatened or stalked, merits investigation. Cyber-Crime can be studied from different perspectives, including an offender's or a victim's perspective. Cyber-Crime is a new domain of research in the field of criminology (Torosyan, 2003). Although research on Internet crime from the offender perspective is growing (Skinner and Fream, 1997; Rogers, 2001; Foster, 2004), there is little if any research concerning the victims of Internet crimes.

In the criminology literature, I access two domains concerning the study of victimization: routine activities and fear of crime. As proposed by Cohen and Felson (1979), routine activities theory proposes that changes in the routine activities of people

explain variation in crime rates. It predicts victimization according to three factors that converge in time and space: motivated offenders, suitable targets, and the absence of capable guardians against a violation. With the advent of the Internet people have changed the way in which they communicate or interact with others, shop, entertain, and do business. I argue that these changes in people's activities, that is use of the Internet, increases the probability that motivated offenders will converge with suitable targets in the absence of guardians. Therefore, a routine activity approach has relevance for my research. Here, I developed measures for suitable target as well as risk exposure that are applicable for the study of Cyber-Crime victimization. One of the Cyber-Crimes investigated in this study is the computer virus. Unlike other cyber crimes, computer viruses are prevalent. So, I created two dependent variables; 1) computer virus victimization alone; and 2) Cyber-Crime victimization, which includes computer virus.

In the fear of crime literature, criminologists believe that fear of crime is predicted by the following variables: gender, age, race, SES, perceived risk, incivilities, and prior victimization. Others suggest that fear of crime affects the intensity of social interaction (Liska and Warner, 1991).

Fear of crime has become an important research topic since the 1960s (Liska et al, 1982; Hale, 1996). From the 1960s to the 1990s over two hundred articles and books appeared concerning fear of crime (Hale, 1996). According to the 1987 General Social Survey, 43 percent of respondents reported that they were afraid to walk alone at night, (Warr, 1991). The growing interest in fear of crime is attributed to concern about the consequences of the fear of crime, including personal anxiety (Hale, 1996). In this study,

I developed a scale for fear of Cyber-Crime, and a measure for perceived seriousness that are valid to the study of fear of Cyber-Crime.

Drawing on these two bodies of literature, fear of crime and routine activities, this dissertation examines the following: 1) How the use of the Internet (routine activity) affects victimization; and 2) the extent to which cyber crime victimization and other factors increase fear of Cyber-Crime.

I use data from the 2004 National Cyber Crime Victimization Survey, which was conducted by the Survey Research Unit, at the Social Science Research Center (SSRC) at Mississippi State University, and funded by the Center for Computer Security Research (CCSR) and the SSRC.

### The Objectives of the Study

The primary objective of this study is to investigate Cyber-Crime victimization among Internet users in the United States by: 1) assessing the factors that impact the victimization of computer virus; 2) assessing the factors that impact the victimization of Cyber-Crime; and 3) predicting fear of Cyber-Crime. Accomplishing this objective will further our criminological understanding of the new phenomenon of Cyber-Crime.

### The Significance of the Study

The significant aspect of this study is that it is the first study to investigate Cyber-Crime victimization among U.S. adults living in households with Internet access. This study makes use of a national survey that is considered to be the first survey that is about Cyber-Crime victimization among U.S. adults living in households with Internet access.

The importance of this study is that it draws attention to the new and growing Cyber-Crime. Cyber-Crime is significant and worth investigation by criminologists because victims of Cyber-Crimes are increasing more quickly than we can detect, arrest, and prosecute cyber-criminals. Roche et al (2003) claim that computer-related crimes are increasing rapidly. Yet, as they claim, criminals of computer-related crime are difficult to detect or trial. Although the growing literature in computer-related crime can be dated back to 1976 (Parker, 1976), research on Internet crime is focused on the offender perspective (Skinner and Fream, 1997; Rogers, 2001; Foster, 2004). There is little if any research concerning the victims of Internet crimes. In criminology, studying victims of traditional crime has become an area of specialization since 1960s and 1970s (Karmen, 1991). This dissertation can contribute to the existing literature of studying victims by broadening the area to encompass victims of Cyber-Crimes who suffer financial loss, and who are threatened or stalked.

Using routine activity and fear of crime perspectives to investigate Cyber-Crime victimization may help us understand Internet behavior as well as factors that impact victimization and fear. The increase in the volume of Cyber-Crime victimization could be explained by changes in people's routine activities of everyday life. With the advent of

the Internet people have changed the way in which they communicate or interact with others, shop, entertain, and do business. These changes in people's activities, that is using the Internet, will increase the probability that motivated offenders will converge with suitable targets in the absence of guardians. Therefore, a routine activity theory can help explain Cyber-Crime victimization.

Routine activity has been used for different purposes. It has been used to foresee property crime, to predict risk of victimization (Messner and Blau, 1987), and to explain trends in crime. Applying routine activity theory to explain Cyber-Crime victimization will enhance our ability to predict as well as explain Cyber-Crime victimization. Besides, it will contribute to routine activity theory by lending support to the theory that will be applied to a wide range of deviant behavior. This contribution, as discussed throughout this dissertation, is made possible through developing different measures of the elements of the routine activity theory to be applied to cyberspace. Suitable targets and risk exposure measures of routine activity will be created and applied to new types of crime, i.e., Cyber-Crime. Doing so, routine activity theory will be able to make the connection between real world crime and cyberspace crime (Yar, 2005).

Fear of traditional crime has become an important research topic since the 1960s (Liska et al, 1982; Hale, 1996). From 1960s to 1990s there were over two hundred articles and books concerning fear of crime (Hale, 1996). According to the 1987 General Social Survey, 43 percent of respondents reported that they were afraid to walk alone at night (Warr, 1991), but, we know little about fear of Cyber-Crime.

Using fear of crime literature to investigate Cyber-Crime helps us to understand whether or not people have developed a fear of Cyber-Crime. If so, how afraid are people of Cyber-Crime? Who are the most likely to be afraid? And, what are the predictors of fear of Cyber-Crime? This dissertation will contribute to the understanding of the fear of crime and will expand the existing literature to include Cyber-Crime, of which victimization is rapidly increasing.

This contribution is made possible through developing different measures of fear of crime. As discussed throughout the dissertation, the fear of Cyber-Crime measure, developed in this study, includes multiple indicators rather than a single indicator. Also, this measure will meet the criteria developed by Ferraro (1995) that refers to a specific crime, Cyber-Crime, and it will tap the state of worry about cyber crime, and will directly assess Cyber-Crime victimization in the subject's everyday using of the Internet. Measure of perceived seriousness is created to be applicable to the fear of Cyber-Crime. Interactions terms of age by gender and victimization by gender are created to examine their effects on fear of Cyber-Crime.

Because fear of crime can reshape people's lifestyle (Warr, 1991) fear of Cyber-Crime could have negative consequences on Internet use. This is very important for policy implication and business. If people have a high level of fear of Cyber-Crime, then it is necessary for all jurisdictions to have trained personnel to investigate and prosecute such crimes. An unpublished study of Law Enforcement and District Attorney Computer

Crime Survey in Mississippi State<sup>1</sup>, 2003, shows that more than half of the sample (n=64; 65.6%) does not have employees with special training and expertise in dealing with computer-related crime. Likewise, about the same percentage (64.1%) of the sample does not have a particular procedure or protocol for dealing with computer-related crime.

E-commerce, selling and buying products and services using the Internet, are all expanding rapidly. If people develop a high level of fear of Cyber-Crime, they may become less likely to use the Internet, and this, in turn, may negatively influence e-commerce, and businesses may lose millions of dollars.

---

<sup>1</sup> This survey is funded through the MSU Center for Computer Security Research with additional support from the MSU Social Science Research Center.



## CHAPTER II

### REVIEW OF THE LITERATURE

#### Cyber-Crime

We have entered a new informational age (i.e., cyberspace or virtual world). People spend part of their daily life in cyberspace, creating and enjoying new types of social relationships, being in touch with the outside world, and doing some business. All of these activities have been made possible for everyone having a computer, a modem and a little technical knowledge. In other words, the Internet is the agent that creates what is now known as cyberspace, or the virtual world.

Cyberspace has unique features, which have, unfortunately, brought about new types of crimes, called Cyber-Crimes. Wall (2005) defines Cyber-Crime as "crimes that are mediated by networked computers and not just related to computers" (P 79). So, Cyber-Crime is crime committed via the Internet such as viruses, cyberstalking, identity theft, fraud, child pornography, hacking, and blackmail, etc.

Cyberspace creates new opportunities for criminals to commit crimes through its unique features. These features are seen by Wall (2005) as "transformative keys" :1) "globalization" enables offenders with new opportunities to exceed conventional boundaries; 2)"distributed networks" generate new opportunities for victimization; 3)"synopticism and panopticism" enables offenders to "servile" their victims remotely; 4)"data trails" create new opportunities for criminal to commit identity theft.

To fully grasp how the Internet generates new opportunities for criminals to commit new Cyber-Crimes, Wall (2005) create a matrix of Cyber-Crimes showing levels of opportunity by type of crime:

Table 1. The Matrix of Cyber-Crime: Level of Opportunity by Type of Crime

	<b>Integrity-related (Harmful Trespass)</b>	<b>Computer-related (Acquisition theft/deception)</b>	<b>Content-related 1 (Obscenity)</b>	<b>Content-related 2 (Violence)</b>
<i>More opportunities for traditional crime (e.g., through communications)</i>	Phreaking Chipping	Frauds Pyramid schemes	Trading sexual materials	Stalking Personal Harassment
<i>New opportunities for traditional crime (e.g., organization across boundaries)</i>	Cracking/Hacking Viruses H activism	Multiple large-scale frauds 419 scams Trade secret theft ID Theft	Online Gender trade Camgirl sites	General hate speech Organized paedophile rings (child abuse)
<i>New opportunities for new types of crime</i>	Spams (list construction and content) Denial of Service Information Warfare Parasitic Computing	Intellectual Property Piracy Online Gambling E-auction scams Small-impact bulk fraud	Cyber-sex Cyber-pimping	Online Grooming Organized Bomb talk/Drug talk Targeted hate speech

Source: Wall, David S. 2005. "The Internet as a Conduit for Criminal Activity." Pp77-98 in *Information Technology and the Criminal Justice System*, edited by April Pattavina. Sage Publications.

As Wall (2005) illustrates, table 1 shows the impact of the Internet on criminal opportunity and criminal behavior. There are three levels of the impact of the Internet on criminal opportunity as shown on the Y-axis of the table. The Internet has created *more opportunities for traditional crime*, such as Phreaking, Chipping, fraud, and stalking.

These types of crime were already existent, but the Internet increases the rate and prevalence of these crimes by creating more opportunities for criminals. Another level of the impact the Internet has on criminal opportunity are *new opportunities for traditional crime*, such as cracking/hacking, viruses, large-scale fraud, online gender trade (sex), and hate speech.

The third level are *new opportunities for new types of crime*, such as spam, denial of service, intellectual property piracy, online gambling, and e-auction scams, and cyber-sex. From this table we can see that the Internet creates new opportunities not only for traditional crimes but also for new crimes that have never been known before. Of the new opportunities for traditional crime, as table 1 shows, is a virus.

A virus is a program or code that replicates itself onto other files with which it contacts. A virus can do harmful things to an infected computer by wiping out databases or files, damaging some important parts in a computer such as Bios, or forwarding a pornographic message to everyone listed in the email address book of an infected computer (Burden et al, 2003). The Internet allows viruses to spread faster through emails and websites. Viruses are made intentionally to carry out certain functions, which are destructive (Britz, 2004).

Because of the harm a virus can cause to infected computers through Internet, it is categorized as a Cyber-Crime (Burden et al, 2003; Wall, 2005; Mannion, 2001). For example, Burden et al (2003) distinguishes between true Cyber-Crime and e-enabled crime. They argue that true Cyber-Crimes are "... dishonest or malicious act, which would not exist outside of an online or at least not in the same kind of form or with anything like the same impact" (P 222). Burden et al (2003) list viruses as one form of true Cyber-Crime. E-enabled crimes, on the other hand, are crimes that existed before the Internet, but increased over the Internet (Burden et al, 2003).

In 2001, David L. Smith was accused of unleashing the "Melissa" computer virus in 1999, causing millions of dollars in damage and infecting numbers of computers and computer networks. He was sentenced to 20 months in a federal prison, and was ordered to serve three years of supervised release after completion of his prison sentence, and was fined \$5,000 ([www.cybercrime.gov](http://www.cybercrime.gov)).

As for the impact of the Internet on criminal behavior, the table shows on the X-axis that there are four types of crime: integrity-related harmful; computer-related acquisition; content-related (obscenity); and content-related (violence). As Wall argues, for each type of these crimes there are three levels of harm: least; middle; and most harmful. So, for example, in integrity-related harmful type, phreaking and chipping is least harmful, whereas denial of service and information warfare is most harmful, as Wall argues.

### *How Cyber-Crime Happens*

A report published by the National White Collar Crime Center (NW3C) (2002) asserts that cyber-space creates new opportunities for criminal to interact with victims. It shows that the unique features of the Internet, which are anonymity and friendly use, provide new ways for criminals to commit their crimes. In addition, the Internet enables criminals to communicate quickly, and efficiently transmit large quantities of information to many victims via chat rooms, e-mail, message boards, or Web sites (NW3C, 2002). All they need are basic computer skills and computers that are connected to the Internet. “Consequently, a single computer provides a diverse medium for conducting an array of crimes. Criminals can use the computer to initiate and maintain contact with potential victims via the Internet, to conduct fraudulent financial transactions, to illegally replicate and/or distribute legitimate products or information, or to co-opt confidential, personal information. Computer crimes frequently overlap each other during their commission” (NW3C, 2002 p 1).

Cyber-Crimes include fraudulent marketing schemes, on-line auctions, work-at-home schemes, gambling operations, and spam (NW3C, 2002 a). As NW3C (2002) indicates, in on-line banking schemes criminals collect confidential personal information by “spoofing a valid Web site, creating a deceptive Web site, or even touting a legitimate sounding scam in a chat room”. When a criminal gets the bank account information, illegal transfers of money, for example, can happen in one quick transaction (NW3C, 2002).

Personal information that is electronically stored on the Internet is subject to theft by criminals, and includes social security numbers, mother's maiden name, bank PIN numbers, or photographs, and has become a marketable commodity (NW3C, 2002 a). The NW3C report claims that criminals can commit identity theft when an Internet user "co-opts" his/her name, or his/her credit card number for their own use. How does it happen? The report shows that:" One method for acquiring personal information occurs when an employee in a position of trust steals confidential information from clients by accessing electronic files. Another means of attaining information is by illegally replicating credit card numbers with a computer during the course of a legitimate business transaction. Often victims of identity theft may never know the person who appropriated their information" (p 1).

Internet fraud is defined by The United States Department of Justice as "...any type of fraud scheme that uses one or more components of the Internet - such as chat rooms, e-mail, message boards, or Web sites - to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme." The advent of the Internet has allowed different types of fraud to occur faster than ever before.

As the United state Department of Justice claims "the same types of fraud schemes that have victimized consumers and investors for many years before the creation of the Internet are now appearing online (sometimes with particular refinements that are unique to Internet technology)"

(<http://www.internetfraud.usdoj.gov/#What%20Is%20Internet%20Fraud>).

There are different types of Internet fraud that could reach to 419 fraud (NW3C , 2002 b). But the major types reported by The United States Department of Justice are: auction and retail schemes online; business opportunity/"work-at-home" schemes online; identity theft and fraud; investment schemes online: market manipulation schemes; and credit-card schemes.

Auction fraud happens when an on-line user buys something from ebay.com, Yahoo.com, or Ubid.com and he or she does not receive the item he or she won. The problem associated with this type of fraud is that, as NW3C (2002 b) indicates, victims have little information about the sellers. All they know is the email address of the sellers (NW3C, 2002 b).

Identity theft is defined by NW3C (202 b) as “ the illegal use of someone’s personal data such as name, social security number, or driver’s license to obtain money, merchandise, or services by deception” (p2). Identity theft includes fraudulently obtaining credit, stealing money from the victim’s bank accounts, using the victim's credit card number, establishing accounts with utility companies, renting an apartment, or even filing bankruptcy using the victim’s name (<http://www.davislogic.com/cybercrime.htm#Cybercrime>).

Stock market manipulation happens when victims try to benefit from an on-line opportunity to increase their money. Criminals can use different methods through spam e-mail or Internet message boards in order to increase prices in traded stocks. When the price doubles or triples, the criminals sell off their holdings for “significant profit

margins”. Victims, on the other hand, are then left with less valued stocks. The Internet can also be used to bring down stock with rumors or lies (NW3C, 2002 b).

Another type of Cyber-Crime is cyberstalking. It is defined by NW3C (2003) as “one individual harassing another individual on the Internet using various modes of transmission such as electronic mail, chat rooms, newsgroups, mail exploders, and the World Wide Web. Cyberstalkers can also obtain personal information about their victims (e.g., home address, phone number) from the Internet and utilize this information to meet their victims in person” (P 1). Cyberstalking takes different forms such as: email that contains threatening message; spamming (in which a stalker sends a victim a multitude of junk e-mail); live chat harassment (online verbal abuse); sending electronic viruses; and tracing another person's computer and Internet activity (The National Center of Victims of Crime:

<http://www.ncvc.org/ncvc/main.aspx?dbName=DocumentViewer&DocumentID=32458>).

Cyberstalking occurs in three ways: through email; Internet; and computer (Ogilvie, 2000). Cyberstalkers are usually male, and victims of cyberstalking are women and children (USDOJ report on cyberstalking;

<http://www.davislogic.com/cybercrime.htm#Cybercrime>; NW3C, 2003). Working to

Halt Online Abuse WHO@<sup>1</sup> reports that 1221 cases were handled by the organization from 2000 to 2004. The demographic information of the victims, as reported by WHO@ are as follow:

---

<sup>1</sup> WHOA is a volunteer organization founded in 1997 to fight online harassment through education of the general public, education of law enforcement personnel, and empowerment of victims (<http://www.haltabuse.org/index.shtml>).



*Age:* forty-eight percent of the victims are in age group of 18-30; twenty seven percent are in age group 31-40; and twenty three percent are older than 40.

*Race:* seventy-eight percent of the victims are Caucasian; 3.5 percent are Hispanic; 3 percent are African-American; and 3 percent are Asian.

*Gender:* Sixty-nine percent of the victims of cyberstalking are female; and eighteen percent are male. 13 percent are unknown.

Hacking is a term that is used to describe computer criminals who break into or harm computers (<http://library.thinkquest.org/04oct/00460/hackingHistory.html>).

Hackers are those who deliberately access computers without authorization regardless of “knowledge or stimulus” (Britz, 2004). Although hacking can be traced back to the 1970s, it is still evolving, and the advent of the Internet made hacking even more dangerous and widespread

(<http://library.thinkquest.org/04oct/00460/hackingHistory.html>). Examples of malicious acts done by hackers are viruses, denial of services, and identity theft. Robert Morris Jr, in 1988, released a worm on the ARPANET system when spread through government and university computer systems and caused between \$5 and \$100 million in damages (Britz, 2004; Hacker History, a web site). Kevin Mitnick, a known hacker, was charged with stealing 20,000 credit card numbers (Schell; and Dodge, 2002). In 2000, hackers launched one of the biggest denial of service attacks, which impacted many websites such as Yahoo and Amazon offline

(<http://library.thinkquest.org/04oct/00460/hackingHistory.html>).

### *Cyber-Crime Victimization*

Cyber-Crimes are on the rise, and the number of Internet crime victims is increasing every year. In 2004 the Internet Crime Complaint Center (IC3) referred 190,143 complaints to enforcement agencies on behalf of individuals. These complaints included many different fraud types such as auction fraud, non-delivery, and credit/debit card fraud, as well as non-fraudulent complaints, such as computer intrusions, spam/unsolicited e-mail, and child pornography. This is a 64.2 percent increase over 2003 when 63,316 complaints were referred. The total dollar loss from all referred cases of fraud was \$68.14 million with a median dollar loss of \$219.56 per complaint.

A 2001 survey by the Computer Security Institute (CSI), shows that 85 percent of respondents (the sample was 538 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities) detected computer security breaches within the prior twelve months. More than 70 percent of the respondents cited their Internet connection as a point of attack, compared to 31 percent who identified their internal systems as a source of attack.

In 2004 there has been an increase in almost every kind of security threat that affects computers. One hundred thousand barriers were broken by known viruses and the number of new viruses increased by more than 50 percent since 2003 (Ward, Mark Technology Correspondent, BBC News website, 2004). Phishing attempts, in which conmen try to trick people into handing over confidential data, recorded a growth rate of more than 30 percent since 2003 and attacks are becoming increasingly sophisticated. Also on the increase are the number of networks of remotely controlled computers, called

bot nets, used by malicious hackers and conmen to carry out many different Cyber-Crimes (Ward, Mark Technology Correspondent, BBC News website, 2004)

The number of Internet users is also increasing. About thirteen percent of the world population is using the Internet. From 2000-2005 there was a 126.4percent increase in Internet usage in the world. In the United States 68.8 percent of the population use the Internet, with an increase of 111.5 percent from 2000 to 2005 (InternetWorldStats.com, 2005).

Many computer users think their systems and their networks are safe. Unfortunately, computers that are connected to the Internet are not safe. If one has a computer and a modem connected to the Internet, it is just like living in a high-crime neighborhood (<http://rf-web.tamu.edu/security/secguide/V1comput/Intro.htm>). The problem is that a modem can be used by hackers to gain access to one's computer system. Due to the nature of the Internet, once a hacker connects to that computer, the hacker can often connect to any other computer in the network (<http://rf-web.tamu.edu/security/secguide/V1comput/Intro.htm>). Another vulnerability of the computer system includes "back doors". These are holes in security left open within a program that can be used by criminals to gain unauthorized access to the system (Britz, 2004). Viruses, Trojan Horses, and Worms all constitute threats to computer systems and most computer systems are not fully immune from them. The antivirus firm McAfee claims that there are more than 58,000 virus threats in existence, and Symantec, antivirus company, claims that 10 to 15 new viruses are discovered each day. Spyware and anti-virus software cannot fully protect computers from new viruses, worms or spy ware

because these software usually are developed as countermeasures after malicious wares have been spread over the Internet.

Consumer Reports conducted a Net survey of online consumers in 2005. Using a nationally representative sample of more than 2,200 households with Internet access at home they found that: 1) about 30 percent of the respondents reported that virus or spyware caused serious problems to their computers as well as financial losses; 2) eighteen percent of those who had a virus had to erase their hard drive; 3) fifty one percent of the sample became very cautious visiting Web sites, and thirteen percent of the sample shop online less; 4) six percent of the sample had sent personal information in response to phishing scams; 5) seventeen percent of the sample did not use anti-virus software; ten percent of those who have high-speed broadband access did not have firewall protection (Consumer Reports, 2005).

#### *Is Cyber-Crime a White-Collar Crime?*

Based on the National Incident-Based Reporting System (NIBRS), of the crimes committed using a computer, forty two percent are White-Collar crimes (Barnett). Also, NIBRS classifies computer crime as a White-Collar crime. Given the features and definition of Cyber-Crime does that lead us to say that Cyber-Crime is a White-Collar crime? Some consider Cyber-Crime as a new type of White-Collar crime (Roche et al, 2003). Before reaching to a conclusion about whether a Cyber-Crime is a White-Collar crime or not, it is plausible to discuss White-Collar crime.

The concept of White-Collar crime was first introduced by Edwin H. Sutherland during his presidential address at the American Sociological Society Meeting in 1939. He defined White-Collar crime as "a crime committed by a person of respectability and high social status in the course of his occupation" (1940, p 9). But this definition has generated many criticisms and attempts to refine it. Some argue that Sutherland's definition of White-Collar crime does not include other crimes that are committed by rich people but not in the course of their occupation (Edelhertz 1970). Shapiro (2001) calls for a definition of White-Collar crime that focuses on offense characteristics rather than offenders.

In an attempt to broaden the concept of White-Collar crime, Marshall Clinard and Richard Quinney (1973) classify White-Collar crime into two categories: occupational and corporate. Organizational crime, advanced by Schragger and Short (1978), is another effort to broaden Sutherland's concept of White-Collar crime. Colman (1994) argues that these new concepts are just "subtypes" of White-Collar crime. He proposes a modified definition of White-Collar crime: "White-Collar crime is a violation of the law committed by a person or group of persons in the course of an otherwise respected and legitimate occupation or financial activity"(1994 p5). This definition is broader than Sutherland's and includes tax evasion and other crimes that are not committed directly in the course of one's occupation (Barkan, 1997).

The definition of White-Collar crime is highly debated among criminologists. Some define it by offender characteristics; others relate it to organizational culture. Yet others define it by offenses. Roche et al. (2003) argue that any definition of White-Collar

crime must include three elements: 1) "crime", that is, an act must violate some statute; 2) "gain" which could be money or any "tangible or intangible" that has a value to a criminal; 3) "deceit", all White-Collar crimes are committed by deception and not by force. Roche et al. claim that the elements found in Sutherland's definition of White-Collar crime, "person of respectability, and "in the course of his occupation" do not apply to a modern analysis of White-Collar crime, and computer crime is a new form of White-Collar crime (Roche et al, 2003).

Roche et al's argument is consistent with the definition of White-Collar crime adopted by the Federal Bureau of Investigation (FBI). The FBI defines White-Collar crime as "those illegal acts which are characterized by deceit, concealment, or violation of trust and which are not dependent upon the application or threat of physical force or violence. Individuals and organizations commit these acts to obtain money, property, or services; to avoid the payment or loss of money or services; or to secure personal or business advantage" (USDOJ, 1989, p. 3.). In this definition there are no mentions of either occupation or offender characteristics.

Edelhertz et al (1977) defines White-Collar crime as "an illegal act or series of illegal acts committed by nonphysical means and by concealment or guile, to obtain money or property, to avoid payment or a loss of money or property, or to obtain business or personal advantage". This definition of White-Collar crime encompasses a wide range of crimes that do not involve physical means. Also, this definition characterizes an illegal act as hidden or guileful for and driven by monetary gain. Cyber-Crime is a crime that is hidden, uses networks (nonphysical means), and sometimes leads to profits.

The nature of Cyber-Crime is that it occurs only through the Internet networked computers. When we take the networked computer (i.e., the Internet) from the *equation*, as Wall (2005) claims, Cyber-Crime wouldn't exist. White-Collar crime, on the other hand, does not require such a condition. Computer facilitates the occurrence of White-Collar crimes but is not the cause of it. Money laundering, for example, is a White-Collar crime. But the computer makes it easy and efficient for a White-Collar criminal to move money (Roche et al, 2003).

Cyber-Crime covers a wide range of crimes, as mentioned above, that are committed using networked computers. Some of these crimes lead to financial gains, such as Internet fraud or scams offering bogus goods or services for money, and identity theft like theft of debit/credit card. Other types of Cyber-Crimes do not lead to profits such as cyberstalking, cyberharassment, viruses, and child pornography.

Recalling the definition of White-Collar crime, which includes property or financial gain, not all types of Cyber-Crime fully integrates into the white-collar crime category. However, some forms or types of Cyber-Crime (those that lead to financial gain) could be considered new types of White-Collar crime because they meet the conditions of White-Collar crime, which are financial gain, deception, and concealment.

Based on the above discussion, Cyber-Crime is a new type of crime that shares some characteristics with White-Collar crime: crime; gain; and deceit. But it has its own unique features: "globalization; distributed networks; synopticism and panopticism; and data trails (Wall, 2005), see figure 1.

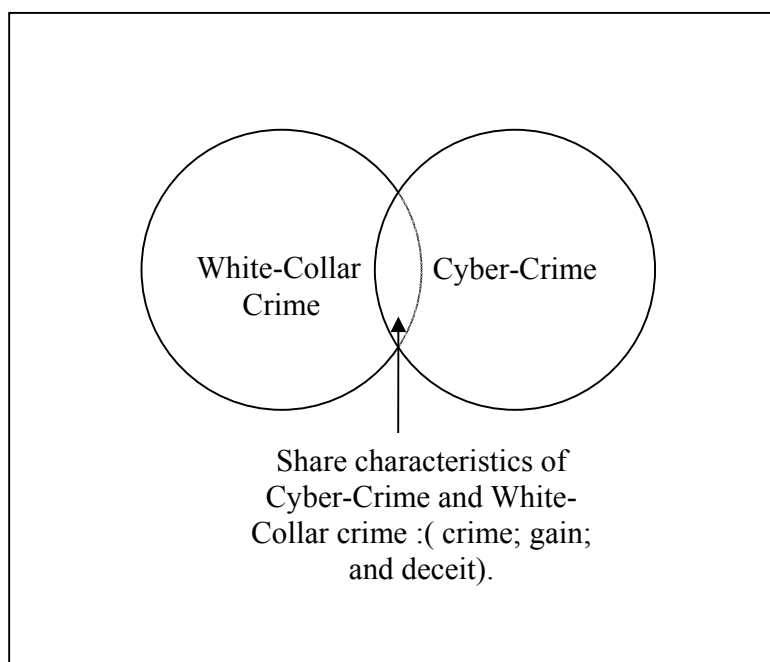


Figure 1. Cyber-Crime and White-Collar Crime Shared Characteristics

### Routine Activity Theory

The increase in the volume of Cyber-Crime victimization could be explained by changes in people's routine activities of everyday life. With the advent of the Internet people have changed the way in which they communicate or interact with others, shop, entertain, and do business. I argue that changes in people's activities, that is using the Internet, will increase the probability that motivated offenders will converge with suitable



targets in the absence of guardians. Therefore, a routine activity approach has relevance for my proposed research.

Routine activity theory, as proposed by Cohen and Felson (1979), suggests that crime is likely to occur when three factors converge. These factors are: motivated offenders, suitable targets, and the absence of capable guardians against violation. Cohen and Felson (1979) argue that these three factors are to be present in order for crime to occur, and the absence of one of these factors is “sufficient to prevent the successful completion of a direct-contact predatory crime” (Cohen and Felson, 1979 P. 589).

Routine activity theory assumes that motivated offenders are a given. The theory pays more attention to the convergence in time and space of the other two factors, that is suitable targets and the absence of capable guardians, and argues that such convergence could lead to a large increase in crime rates without any change in the “situational condition” that motivates offenders (Cohen and Felson, 1979). The basic principle of the theory is that structural changes in routine activity affect the convergence of the three elements of the theory, and hence influence the crime rate (Meithe et al, 1987).

The significant implication of the theory is that illegal activities “feed upon” legal activities (Cohen and Felson, 1979). That is, there is a symbiotic relationship between legal and illegal activities (Messner and Blau, 1987). Routine activity theory has been used for different purposes. It has been used to foresee property crime, to predict risk of victimization (Messner and Blau, 1987), and to explain trends in crime.

As Mustaine and Tewksbury (2002) claim, the strength of routine activity theory is based on the idea that crime does not randomly occur in a society, but rather it

“... follows regular patterns regarding situation and behavior, and it examines how these interact with individual characteristics and behaviors” (P 90).

Although routine activity theory has gained popularity as an approach to test the trend in crime rates, there are few empirical studies to further test and develop its elements. In general, although routine activity is applied in predicting different types of crime, it is more predictive of property crime than personal crime (Meithe, Stafford, and Long 1987; Stahura and Sloan III, 1988; Bennett, 1991; Rodgers; and Roberts, 1995). So, according to Bennett (1991), routine activity is a “crime-specific” theory.

Meithe et al (1987), using a sample of 107,678 residents in thirteen U.S cities, tested the effect of routine activity variables (risk exposure: daytime and nighttime activities) on whether or not a respondent was a victim of violent crime and whether or not property crime victimization was reported. They found that routine activities variables have direct and mediating effects on property victimization, and not violent crime.

Cohen et al (1981) tested the effect of routine activity variables (i.e., exposure, proximity and guardianship) on criminal incident (burglary, assault, and or personal larceny). Using National Crime Survey (NCS) of households in U.S, they found that routine activities variables have a significant effect on predatory victimization.

Stahura and Sloan III (1988), in their study, measured suitable target as “percent multiple housing structure”, and number of retail, wholesale, service and manufacturing establishments in the suburbs. They operationalized guardianship as “police employment, and female labor force nonparticipation”. They found support for routine

activity theory. Routine activity variables predicted property crime especially when they were entered as multiplicative terms in the model (Stahura and Sloan III, 1988).

Fisher et al (1998) applied routine activity theory to predict theft and violence victimization. They found that routine activity variables (exposure, attractiveness, proximity to crime, and the lack of guardianship) have significant effects on predicting property victimization. As for violent crime victimization, they claim that the main effects included the participating in partying at night and using drugs.

Messner and Blau (1987) apply routine activity theory to test the relationship between macro-level indicators of leisure activities and violent crime. Using a sample of Standard Metropolitan Statistical Areas (SMSA), they found that leisure activities that take place within the home have a negative relation with crime rates, whereas leisure activities that take place away from the home have a positive relation with crime rates.

When predicting a specific crime, routine activity appears to have explanatory power. Predicting female sexual assault by using routine activity generates mixed results. Whereas Rodgers and Roberts (1995) found that routine activity variables are poor predictors of women sexual assault, Mustaine, and Tewksbury (2002) found that exposure and proximity as routine activity variables have an effect on sexual assault. Moreover, in conducting a study about stalking among college women, Fisher, Cullen, and Turner (2002) found support for routine activity (risk exposure) in predicting stalking victimization. Similarly, Mustain, and Tewksbury (1999), in an earlier study, found support for routine activity in predicting women's stalking victimization among university women.

Two elements in the routine activity approach are tested in this research: suitable target and risk exposure. Consequently, it is necessary to discuss how they are measured in the literature.

As proposed by the routine activity theory, a victim may be absent from the sight of the crime (Felson and Clarke 1998). In Cyber-Crime victimization, therefore, those whose identity information and credit or debit card numbers are electronically stored on the Internet are always absent or have no control over them. Identity information and credit/debit numbers are the suitable targets and the absence of the possessor makes them easy targets.

Cohen and Felson (1979) claim that four elements characterize suitable targets, which increase the risk of victimization: value, inertia, visibility, and access (P 595). Identity information and credit/debit card numbers are valuable for offenders to steal and profit from. Inertia refers to the weight of an item. Identity information and credit/debit card numbers are weightless, which increases the likelihood of being stolen. Visibility indicates the exposure of a suitable target to an offender (Cohen and Felson 1979). The Internet is replete with many commercial websites that sell and buy different goods. Thus, identity information and credit/debit card numbers are visible to offenders. As for accessibility, identity information and credit/debit card numbers are accessible by offenders (i.e., hackers).

Suitable target is measured in various ways in studies that test routine activity theory. Cohen et al (1981) differentiates suitable target as “*target attractiveness*” based

on two types of motivation: instrumental and expressive\*. They argue that when crime is motivated by an instrumental goal, then the more attractive the target, the higher the risk of victimization (Cohen et al 1981). Although they did not deny expressive motivation they assume that most property crime is committed for instrumental ends. In Cyber-Crime victimization, however, not all Cyber-Crime is committed for instrumental ends. Some virus attacks and hacking, for example, are committed only for thrill-seeking, i.e., expressive ends. Marjie T. Britz (2004) categorizes hacking by motivation. One of these categories is “informational voyeurism”. The motivation of these individuals ranges from curiosity to “sensationalism”.

Stahura and Sloan III (1988) operationalized suitable target as “percent multiple housing structure, and number of retail, wholesale, service and manufacturing establishments in the suburbs” (p1107). They claim that these multiple housing units and business establishments provide more targets for potential offenders. Living in multiple housing units allows residents to be well-informed about what is available for them and how it could be taken. In Cyber-Crime victimization certain websites provide offenders with good information about where to find identity information and credit/debit card numbers as suitable targets.

Fisher et al (1998) use an attractiveness dimension of suitable target. In their research they measured suitable target in terms of “possession of cash”. They asked respondents how much money they spent on entertainment, recreation or restaurants.

---

\* “Instrumental means the act is a means of acquiring something one desires. Expressive refers to the act of attacking a person or stealing property is the only reward sought in doing so” (Cohen, et al 1981 p508).

In summary, two dimensions of suitable target are discussed in the literature: attractiveness (i.e., value) and accessibility. But the other two dimensions (i.e., inertia, and visibility) weren't discussed explicitly. In Cyber-Crime victimization, all the suitable target dimensions apply to identity information and credit/debit card numbers.

The other element that is applicable to the current research is risk exposure. Routine activity suggests that exposure to certain places at certain times increases victimization risk (Cohen and Felson 1979). The victimization literature has shown that risk victimization increases when people spend more time in public places. Cohen et al (1981) define exposure as "the physical visibility and accessibility of persons or objects to potential offenders at any given time or place" (p 507). They measured exposure indirectly by creating seven categories of social demography of the respondents<sup>3</sup>. They believe that such categories reflect differences in the level of exposure to victimization (Cohen et al 1981). Fisher and Turner (2002) measured risk exposure by sorority membership and substance use

Risk exposure has been measured directly by the nature and quantity of activities outside the home. Meithe et al (1987) measure risk exposure by "frequency of nighttime entertainment" and day activity outside the home. They believe that daytime activity outside the home (i.e., work or school) creates patterns that are predictable by offenders.

Mustaine and Tewksbury (1998, 2000) measured risk exposure by frequency of time spent alone, with strangers or away from home in weekdays and weekends. Rodgers

---

<sup>3</sup> These categories are: "1) not married and employed; 2) not married and unemployed; 3) not married and not in the labor force; 4) married with husband and wife employed and no children; 5) married with both husband and wife employed with children; 6) married with head of household employed and wife (or husband) of head not in the labor force; and 7) married with head of household unemployed" (Cohen et al 1981, p515).

and Roberts (1995) measured risk exposure by frequency of using public transportation alone after dark and walking alone after dark. In Cyber-Crime victimization, frequency and duration of Internet use determines the amount of time spent on the Internet, which is believed to be a high risk place.

Based on a review of the routine activity literature, I propose that Cyber-Crime victimization can be predicted by the routine activity approach.

Table 2. Routine Activity & Cyber-Crime Victimization

	Routine Activity		
	Location of offenses (risk exposure)	Suitable target	Guardianship
<b>Cyber-Crime Victimization</b>	<i>On-line activities entail high risk of victimization</i>	<i>Personal information; credit card #</i>	<i>Anti-virus, anti- spam, and anti-spy software (all not guaranteed)</i>

As table 2 shows, the Internet is a place that presents a high risk of victimization. As mentioned above, in 2004 IC3 referred 190,143 complaints including different fraud types such as auction fraud, non-delivery, and credit/debit card fraud, as well as non-fraudulent complaints, such as computer intrusions, spam/unsolicited e-mail, and child pornography. Also, the Federal Trade Commission (FTC), in 2004, reported that a total of 388,603 of the Consumer Sentinel complaints were fraud-related, of which 205,960 (53percent) complaints were Internet-related.

The suitable targets on the Internet that are valuable, attractive and at high risk of illegal use are personal information and credit card numbers that are stored on the

Internet. As for guardianship, the Internet provides no protection against any fraud or identity theft whatsoever. As mentioned before, Spyware and anti-virus softwares cannot fully protect computers from new viruses, worms or spy ware because these software usually are developed as countermeasures after malicious wares have been spread over the Internet.

To illustrate Felson (2002) claims that to understand crime it is necessary to visualize it as a setting, in which people “converge or diverge” to influence opportunities for crime. The crime setting contains, as Felson argues, necessary elements. These elements are: motivated offender, suitable targets, and the lack of capable guardianship. Figure 2 illustrates the Internet as a Cyber-Crime setting where the motivated offender (e.g., a hacker) and suitable target (i.e., id-target, and money-target) are in the scene. But, capable guardian (i.e., anti-spy and anti-virus software) is out of the setting, as the arrow in the figure shows. As discussed above, anti-virus and anti-spy software cannot fully protect computers from getting infected by virus or spy-ware (e., I., Trojan horse).



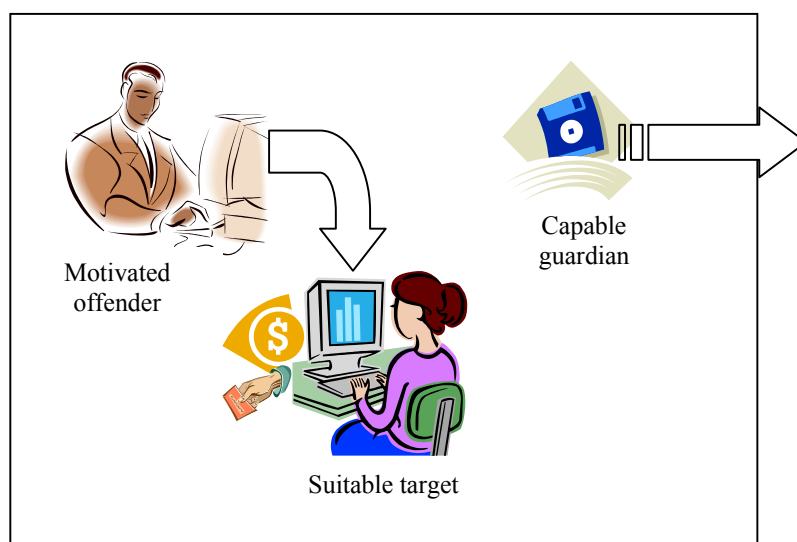


Figure 2. Cyber-Crime Setting. Adapted from Felson, Marcus. (2002). *Crime and Everyday Life*

### Fear of Crime

With an increasing number of Internet users, increasing rate of Cyber-Crimes, and increasing vulnerability of computer systems, victims of Internet crime are expected to increase. Will this lead to increasing fear of Cyber-Crime?

Fear of crime has become an important research topic since the 1960s (Liska et al, 1982; Hale, 1996). From the 1960s to 1990s there were over two hundred articles and books concerning fear of crime (Hale, 1996). According to the 1987 General Social Survey, 43 percent of respondents reported that they were afraid to walk alone at night, (Warr, 1991). The growing interest in fear of crime is attributed to concern about the consequences of the fear of crime, including personal anxiety (Hale, 1996).

Fear of crime is defined as “an emotional response of dread or anxiety to crime or symbols that a person associates with crime.” Ferraro and La Grange (1987), whereas perceived risk “refers to people’s assessments of crime rates and the probability of victimization.” These two concepts received much attention. Fear of crime entails an emotional response, whereas perceived risk entails cognitive judgment. So, each concept is predicted by different variables. To perceive a risk of victimization doesn’t mean a person is afraid of crime.

Ferraro and LaGrange (1987) develop a taxonomy (adapted from the work of DuBow, 1979) to differentiate risk from fear:

Table 3. Taxonomy of Crime Perception

Level of Reference	Type of Perception		
	Cognitive Judgments	Values	Affective Emotions
<i>General</i>	Risk to others; crime or safety assessments	Concern about crime to others	Fear for other’s victimization
<i>Personal</i>	Risk to self; safety of self	Concern about crime to self; personal intolerance	Fear for self victimization

Source: Ferraro, Kenneth F., and Randy LaGrange. 1987. “The Measurement of Fear of Crime” *Sociological Inquiry* 57: 70-101.

According to Ferraro and LaGrange (1987), level of perception ranges from general to personal, and the type of perception varies from cognitive to affective.

“Judgments” is an estimation of the rate of victimization, and it is subjective (Ferraro and LaGrange, 1987). “Values” is a concern about crime, whereas “emotions” reflects fear

(Ferraro and LaGrange, 1987). Ferraro and LaGrange (1987) claim that most researchers ignore this taxonomy and refer to fear of crime as essentially a measure of “judgments” or “values”.

Warr (1984), and Warr and Stafford (1983) developed a different measure of fear of crime. They measure fear of crime with the question ““how afraid you are about becoming the victim of each type of crime in your everyday life”<sup>4</sup>. Also they developed another measure for perceived risk “for each type of crime how likely you think it is to happen to you during the next year”. The improvement they added to the measure of fear of crime was that they refer to specific types of crime.

One problem in measuring fear of crime is a confusion between fear and risk perception (Meithe and Lee, 1984; Hale, 1996; Ferraro and LaGrange, 1987). Most researchers when measuring fear of crime use either the General Social Survey (GSS), or the National Crime Survey (NCS). In the GSS the question used to measure fear of crime is “Is there any area right around here-that is, within a mile- where you would be afraid to walk at night” (Clemente and Kleiman, 1977; Ortega and Myles, 1987). Although this measure is the most commonly used in the literature (Ferraro and LaGrange, 1987), it has also been criticized for not including or mentioning crime (Ferraro, 1995). In the NCS, fear of crime is measured by the question: ““How safe do you feel or would you feel

---

<sup>4</sup> These types of crime are: 1) being threaten with a knife, club or gun; 2) receiving an obscene phone call; 3) having something taken from you by force; 4) being cheated or conned out of your money; 5) being beaten up by a stranger; 6) being approached by people begging for money; 7) being murdered; 8) having strangers loiter near your home ate at night; 9) being raped; 10) being sold contaminated food; 11) having someone break into your home while you are away; 12) being beaten up by someone you know; 13) having your car stolen; 14) being hit by a drunken driver while driving your car; 15) having a group of juveniles disturb the peace near your home; 16) having someone break into your home while you are home (Warr. 1984; Warr and Stafford, 1938).

being out alone in your neighborhood at night (during the day)” (Allen E. et al, 1982, 1988). This measure is also criticized for not distinguishing fear from perceived risk (Ferraro, 1995).

Although there is agreement that fear of crime is a social problem, there is no consistency regarding the predictors of this fear (Clemente and Kleiman 1977), which could stem from the ambiguity in measuring fear of crime (Ferraro and LaGrange, 1987; Hale, 1996; Rountree and Land, 1996; Rader, 2004). The variables that are most commonly used in studies to predict fear of crime are; age, race, gender and social economic status SES. In general, studies suggest that fear of crime is higher among elderly people, females, nonwhites, (Ortega and Myles, 1987) and among lower class respondents (Liska et al 1988).

Clemente and Kleiman (1977) used two national samples from 1973 and 1974 (n= 2,700) to test the effect of race, gender, age, SES, and community size on fear of crime. Using Multivariate Nominal Scaling (MNA) they found that gender and city size were the strongest predictors of fear. Age, race, and SES were less important in predicting fear. Gender has been the best predictor of fear in all studies (Hale, 1996; Liska et al, 1988). Females show a higher level of fear than males (Warr, 1984; Ortega and Myles, 1987). However, gender seems to work different with age. In other words, there is an interaction effect between gender and age. The effect of gender on fear of crime is strong for young people, but diminishes with age (Liska et al, 1988). Warr (1984) found that the effect of the age-gender interaction on fear of crime was significant for ten offenses he examined.

However, Ortega and Myles (1987) found that the age-gender interaction is not statistically significant.

The effect of age on fear of crime is not consistent across studies. Some find that age has a positive relationship with fear of crime (Warr, 1984). Others find that age has a negative relationship with fear of crime (Rountree and Land, 1996). Yet, other studies find no significant effect of age on fear of crime (Ortega and Myles, 1987; Liska et al, 1988). Such discrepancy could result from using different measures of fear of crime. Studies that find a positive relationship between age and fear of crime use global measure of fear, whereas studies that use crime specific-fear find a negative relationship.

Randy L. LaGrange, Kenneth F. Ferraro, and Michael Supancic (1992) conducted a study on perceived risk and fear of crime, and examined the effect of incivilities (physical and social) on both perceived risk and fear of crime. The data are derived from Fear of Crime in America survey sponsored by AARP Andurus Foundation. The sample consists of 1,101 adults. They measure incivilities by respondent's perception of, rather than objective measures, of neighborhood disorder. They developed two measures of incivilities: social incivilities, which include bad neighbors, unsupervised youth, too much noise, and drunk in public. Physical incivilities include trash and litter, loose dogs, graffiti, vacant houses, and abandoned cars (LaGrange et al, 1992). Using multivariate analysis they found that incivilities has a stronger effect on risk perception than on fear of crime, but when they include perceived risk in their model incivilities has no significant effect on fear of crime.

Rountree and Land (1996) examine the dimensions of fear of crime by comparing perceived risk with burglary-specific fear. The data they used were derived from victimization survey data which was a part of a larger crime research project in Seattle, Washington. Using hierarchical logistic regression modeling, they found, contrary to the literature, that young people and whites are more fearful of burglary. Income, as a target attractiveness surrogate, has a negative effect on risk perception, and no effect on burglary-specific fear. Also, they found that sociodemographic variables such as age, gender, and race have different effect on fear of crime and perceived risk. They argue that, contrary to the fear of crime literature, younger people and whites are found to be more fearful of burglary, but gender has no effect on fear of burglary (Rountree, and Land 1996). Age, on the other hand, has very little effect on perceived risk, but gender has a significant effect on perceived risk. That is, males are found to be less likely to feel unsafe than women (Rountree, and Land 1996). As for routine activities and previous experience with burglary, they found that both have effect on perceived risk and fear of crime. But, they argue that routine activities have a weak effect on perceived risk (Rountree, and Land 1996).

Taking a different direction in studying fear of crime Warr and Elisson (2000) introduced the concept of “altruistic fear”. They argue that fear that people have for others in their lives (altruistic) is more common and intense than personal fear. The data they used come from the Texas Poll. The sample consists of 1006 respondents that were interviewed over the telephone (CATI). They found that men are more vulnerable than

women to altruistic fear when it comes to their wives and children (Warr & Elisson 2000). Altruistic fear, they argue, declines throughout the life course.

Victimization as a predictor of fear of crime has generated conflicting results. Some researchers suggest that those who have been victimized are more fearful of crime (Smith and Hill, 1991). Others find a weak relationship (Garofalo, 1979; Liska et al, 1988), yet others find no relationship between victimization and fear of crime (Hill et al, 1985; Joseph, 1997). Carl Keane (1995) claims that the victimization-fear of crime relationship exists when it involves certain offenses and offenders. The sample he used was from the Canadian Violence Against Women Survey.

Knowing someone who was victimized is another explanatory variable in fear of crime. Some found an effect of indirect victimization (knowing someone who was victimized) on fear of crime (Box et al, 1988; Tyler, 1980). Others found no effect of indirect victimization on the fear of crime (Joseph, 1997). Knowing about victimization from someone, a relative or a neighbor provides one's mind with full scope about crime. This leads a person to reinforce his or her sense of vulnerability to victimization (Hale, 1996).

The term perceived seriousness has been used as a predictor of fear of crime (Warr, 1984; Smith and Hill, 1991). Warr (1984) measured perceived seriousness by asking respondents to rank crime seriousness on a scale of 0 to 10. Using a sample of 339 cases from a mail survey, Warr (1984) found that the more serious a crime is perceived, the faster fear is increased. But, Smith and Hill (1991) used the term perceived seriousness as a mediating variable between victimization and fear of crime.

They measure perceived seriousness by asking respondents about how they felt about seriousness of ten types of crimes (0= not a problem; 2= a serious problem). Using a sample of 3109 cases from mail survey, they found that perceived seriousness of crime is positively related to fear of crime.

In another attempt to predict fear of crime, Warr and Stafford (1983) introduced the concept of proximate causes of fear. They argued that fear of crime is a multiplicative product of perceived risk and perceived seriousness (Warr and Stafford, 1983). They measured perceived seriousness by asking respondents to rank crimes on how serious they are on a scale of 0 to 10. Likewise, they measured perceived risk by asking respondents to rank each crime on a scale of 0 to 10 on how likely a crime will occur to them during the next year. They claim that perceived seriousness could predict fear of crime better when it interacts with perceived risk.

In summary, fear of crime is conditioned by the following variables: gender, age, race, SES, perceived risk, incivilities, and victimization. The literature on fear of crime shows that the measurement of fear of crime centers around two questions used in the GSS and the NCS. Both questions, as discussed above, suffer from conceptual shortcomings. Also, most of the studies use only a single indicator of fear of crime rather than multiple indicators. Such indicators do not allow for reliability tests to make sure that the measure of fear of crime is a valid measure.

Kenneth F. Ferraro (1995) suggests that to develop a valid measure of fear of crime a researcher has to take into consideration the following issues: 1) a measure of fear of crime should include emotional states or worry; 2) it should refer to the type of



crime or victimization; 3) it should be directed to assess the “phenomena in the subject’s everyday life; 4) it should include “a range of seriousness for victimizations”.

Based on the above fear of crime literature review and following Ferraro’s schemes of measuring fear of crime I created a measure of fear of Cyber-Crime. This measure includes multiple indicators rather than a single indicator. Also, this measure will meet the criteria developed by Ferraro (1995) in that it refers to a specific crime, i.e., Cyber-Crime, it will tap the state of worry about cyber crime, and it will directly assess Cyber-Crime victimization in the subject’s everyday using of the Internet.

#### Cyber-Crime Victimization and Fear of Cyber-Crime

As discussed above, the growing interest in fear of crime is attributed to concern about the consequences of the fear of crime, including personal anxiety (Hale, 1996). The link or relationship between fear of crime and victimization is a reciprocal. Liska; and Warner (1991) based their research on the claim that fear of crime affects negatively social interaction, which decreases opportunities for crime. Using National Crime Survey (NCS) dataset, they found that robbery positively affects fear, which, in turn, constrain social interaction and reduces opportunities for other crimes. An earlier study by Liska et al (1988) found that fear of crime constrained social behavior.

Victimization increases fear of crime because of the negative consequences it may cause for the victims. Fear of crime reduces people’s social interaction by causing them to stay home and be prisoners of their homes (Liska, and Warner, 1991). Staying home

may work as a guardian for ones own property. So, the opportunity for committing crime is reduced.

Similarly, as discussed in chapter VI, victimization by Cyber-Crime increases the levels of fear of Cyber-Crime, which negatively affects victimization through constraining the behavior of Internet users. Constrained behavior in the context of Cyber-Crime includes the following:

1. Frequency: when people develop high level of fear of Cyber-Crime they might, as a reaction, log on the Internet less frequently.
2. Duration: people who are fearful of Cyber-Crime may limit their staying online.
3. Id-target: people who become fearful of cyber crime might be less likely to enter their personal information on the Internet.
4. Money-target: when people develop high level of fear of Cyber-Crime they might, as a constrained behavior, refrain from entering their credit or debit card numbers to buy or shop on the Internet.

These various types of constrained behavior are assumed to reduce Cyber-Crime victimization.

## Hypotheses

To accomplish the objective of the study and answer the study questions the following hypotheses are examined:

### Computer Virus Victimization and Cyber-Crime Victimization (Routine Activity Application):

H1: It is expected that the more frequently one accesses the Internet the more likely he or she will be victimized, controlling for other relevant predictors.

H2: It is expected that the longer one stays online the more likely he or she will be victimized.

H3: It is expected that respondents whose children use the Internet will have a higher risk of victimization.

### Cyber-Crime Victimization (Routine Activity Application):

H4: It is expected that activities on the Internet that involve divulging personal information will increase victimization.

H5: It is expected that activities on the Internet that involve divulging personal financial information (i.e., credit card) will increase victimization.

### Fear of Cyber-Crime (Fear of Crime Application):

H6: Those who know someone who has been victimized will have higher levels of fear of cyber crime.

H7: It is expected that females will exhibit higher levels of fear of Cyber-Crime than males.

H8: It is expected that respondents whose children use the Internet will have higher levels of fear of Cyber-Crime.

H9: As fear of crime literature suggests, it is expected that those who think that Cyber-Crime is a serious crime exhibit higher level of fear of Cyber-Crime than those who do not.

H10: Those who have experienced prior Cyber-Crime victimization will have higher levels of fear of cyber crime, controlling for other relevant predictors.

## CHAPTER III

### METHODOLOGY

The purpose of the study is to investigate Cyber-Crime victimization among Internet users in the United States by: 1) assessing the factors that impact the victimization of computer virus; 2) assessing the factors that impact the victimization of Cyber-Crime; and 3) predicting fear of Cyber-Crime. Here, I demonstrate the methodological procedures that I adopt in this study.

#### Data

The data for this study was obtained from the 2004 National Cyber Crime Victimization Survey, which was conducted by the Survey Research Unit, Social Science Research Center (SSRC) at Mississippi State University, and which was funded by the Center for Computer Security Research (CCSR) and the SSRC.

Data collection for the 2004 National Cyber Crime Survey was done via telephone interviews with a sample of U.S. adults living in households with Internet access. The interviewing for this survey was conducted in October and November 2004. Households were randomly selected from a national list of people who said they had “Internet access”. The list was obtained from Survey Sampling Inc. (SSI), from their

LITe (low incident population) sampling frame. It is not a probability sample of all US households with telephones<sup>1</sup>.

Within a household the interviewer asked for (and interviewed) an adult (over 17 years old) who uses the Internet. Of the households contacted, 1,207 completed the interview (84.35 percent as a response rate), and 224 refused to participate.

Using dummy coding for some variables, listwise deletion, and deleting four outlier cases resulted in reducing the sample size from 1207 to 987 cases.

### Operational Measurement

Based on the objectives of the study, three dependent variables were created: computer virus victimization, Cyber-Crime victimization, and fear of Cyber-Crime. Computer virus and Cyber-Crime variables are both intended to examine victimization. Although computer virus is considered one type of Cyber-Crime, as discussed in the literature review, it is examined independently in this study for the following reasons: 1) it is more prevalent than the other types of Cyber-Crime; 2) the nature of it does not include crime intent, although it is considered vandalism. In Cyber-Crime victimization measure, I included computer virus as one of the Cyber-Crime types. The reason for this is that only 7.6 percent of the respondents reported that they were victimized by the other types of Cyber-Crime (internet fraud or scam offering bogus goods or services for money ; identity theft like theft of your debit/credit card or social security number; securities

<sup>1</sup> SSI LITe sample are efficient for targeting low incidence population. Having 50 million records, LITe use self-reported technique to collect demographic and behavioral information at individual and household level. LITe samples are taken from sampling frame that is a subset of all US households. Unlike lists, LITe samples are more accurate because they “take into consideration geographic distribution, proper sampling interval, and basic sampling techniques and controls” ([http://www. Surveysampling.com](http://www.Surveysampling.com)).

fraud or stock manipulation; cyber-stalking or cyber-harassment; extortion or blackmail via Internet ; and computer hacking), whereas 61.2% of the sample reported that they were victimized by computer virus. So, excluding computer virus from the Cyber-Crime measure, would result in having a very low variation in the dependent variable, which, in turn, would not allow to predict Cyber-Crime victimization.

#### *Computer Virus Victimization*

Computer virus victimization, as a dependent variable, is whether or not a respondent was a victim of computer virus. The question in the survey was:

Have you ever received a computer virus over the Internet?

The response was: 1= yes; 2= no. Since this variable is a category, I recoded it into a dummy variable. That is, 1= yes; and 0=no.

#### *Cyber-Crime Victimization*

Cyber-Crime Victimization, as a dependent variable, is whether or not a respondent was a victim of a Cyber-Crime. Cyber-Crime includes computer virus, Internet fraud or scam, identity theft, Securities fraud or stock manipulation, cyber-stalking or cyber-harassment, extortion or blackmail via Internet, and computer hacking.

The questions in the survey were:

1. Have you ever received a computer virus over the Internet?
2. Have you ever been the victim of a computer—related fraud or crime?

If so, which of the following has happened to you?:

- a. Internet fraud or scam offering bogus goods or services for money
- b. Identity theft like theft of your debit/credit card or social security number
- c. Securities fraud or stock manipulation
- d. Cyber-stalking or cyber-harassment (via email for example)
- e. Extortion or blackmail via Internet
- f. Computer hacking (computer damage by amateur hackers)

The responses of these questions were 1= yes; and 2=no.

This variable is measured by three steps:

1. Recoding the responses into 1=yes; and 0=no.
2. Creating a count variable by adding up only the value 1 in each variable, which are question 1, and question 2a to 2f. The values in the count variable ranges from 0 to 3.

Cyber-Crime victimization variable could be considered as a count variable, and Poisson regression is preferred when the outcome is count (Neter et al, 1996; Agresti, 2002). I tried to apply Poisson regression using STATA, a statistical package, but it did not work. The dependent variable is highly skewed to the zero values, which results in a very poor fit of the model. So, I had to apply the third step:

3. Dummy coding the count variable into 0=no; and 1and above =1.

### *Fear of Cyber-Crime*

As a dependent variable, fear of Cyber-Crime is measured by the following items:

”How concerned are you.....”



- That you might receive a virus that would damage your computer system.
- That your computer might be accessed/hacked by other users.
- About entering your debit or credit card numbers over the Internet.
- That you might become a victim of a computer—related crime.

Respondents expressed their answers on a three-point Likert scale:

(1) Not at all concerned; (2) Somewhat concerned; (3) Very concerned.

A single composite measure was created consisting of all the four items with an eigenvalue of 2.370 (Cronbach's alpha=0.765). Using explanatory factor analysis, these items are saved as a regression variable (see chapter IV).

Factor analysis is used to identify underlying factors that explain the pattern of correlations within a set of observed variables. Factor analysis is often used in data reduction to identify a small number of factors that explain most of the variance observed in a much larger number of manifest variables.

### *Frequency*

As hypothesized, to predict Cyber-Crime victimization, the more frequently one accesses the Internet the more likely he or she may be victimized. So, this variable is measured by asking respondents the following question:

On average, how often would you say you get on the Internet at home?.

0= Never

1= A few times per year

2= Once or twice a month

3= Once or twice a week

4= Several days a week

5= Once a day

6= Several times each day

### *Duration*

This variable measures the amount of time spent on the Internet. So, the variable, Duration, is assessed by asking respondents the following question:

When you use the Internet at home, how long do you usually stay online at one time?

1= 30 minutes or less

2= 1 hour

3= 1-2 hours

4= 2-3 hours

5= 3 or more hours

### *Id-target and Money-target*

As routine activity theory suggests, target suitability characteristics include value, visibility, and accessibility (Cohen and Felson, 1979). Id numbers, i.e., personal information, and money-target, i.e., credit and debit card numbers, stored on the Internet are valuable and easily accessible. So, the Id-target variable is measured by creating a count variable that adds only value 1 of the following items:

- Which of the following have you done using the Internet?: (1= yes; 0= no)

- Researched cars you might buy
- Advertised a car you want to sell
- Taken a web-based class for high school or university credit
- Used an on-line auction site
- Set up a web page
- Looked for jobs/employment
- Looked to hire someone

The values in the id-target variable ranges from 0 to 7 with mean = 2.348 and SD=1.5.

Money-target is measured by creating a count variable that adds only value 1 of the following items:

- Which of the following have you done using the Internet?: (1= yes; 0= no)
  - Bought airline tickets or hotel rooms
  - Rented a car
  - Bought books, movies, or music
  - Bought or had flowers sent
  - Paid bills (electricity, phone, gas, etc.)
  - Bought a car

The values in the money-target variable ranges from 0 to 6 with mean = 1.825 and SD=1.47.

### *Knowing Victim*

As hypothesis five states, those who know someone who has been victimized may have higher levels of fear of Cyber-Crime. This variable is measured by the following question:

Has one of your family members or friends ever been the victim of a computer-related crime?

Respondents expressed their answer by (1= yes; 0= no).

### *Having Children with Access to the Internet:*

As the fear of crime literature suggests, fear that people have for others in their lives (altruistic) is often more common and intense than personal fear. So, those who have children are expected to be more fearful of Cyber-Crime than those who do not.

This variable is measured by the following question:

Do any of your children use the Internet to access websites?

Respondents expressed their answer by (1= yes; 2= no).

Because of missing data this variable has, I applied the following procedure to save such missing data:

- 1) I recoded this variable such that (1=yes; 0=no)
- 2) I created a missing category.
- 3) I dummy coded this variable such that: 1=yes; 1=missing; 0=no.

### *Perceived Seriousness*

In fear of crime literature, the effect of perceived seriousness of crime on fear of crime is implied or given by its nature. But, Warr and Stafford (1983), as mentioned in the review of the literature, point out the effect of this variable and measure it by asking respondents to rank crime seriousness on a scale of 0 to 10. They claimed that perceived seriousness when combined with perceived risk could predict fear of crime. Smith and Hill (1991) measured perceived seriousness of crime by asking respondents about how they felt about seriousness of ten types of crimes (0= not a problem; 2= a serious problem). Since perceived seriousness of Cyber-Crime has never been estimated on the literature, and since perceived seriousness has shown an impact on fear of crime (Smith and Hill, 1991; Warr and Stafford, 1983), I provide a tentative measure of it and include it in the equation of fear of Cyber-Crime.

Therefore, a measure of perceived seriousness is created from the following survey question: “Persons convicted of committing computer-related crimes are not punished as severely as they should be”. Respondents expressed their answers on four-point Likert scale: (1) strongly agree; (2) somewhat agree; (3) somewhat disagree; (4) strongly disagree. This measure has a face value, and it refers to all types of Cyber-Crime.

Because the perceived seriousness variable is skewed, I recoded this variable into a dummy variable. That is, strongly agree and somewhat agree=1; somewhat disagree, and strongly disagree=0.

### *Gender*

The Fear of crime literature shows that females are more fearful of crime than males. The respondents' gender is measured by asking the question: What is the respondent's gender? (1=male; 2= female) and it is used as a dummy variable such that (female=1; male=0).

### *Race*

The respondents' race is measured by asking the question: What is your race or ethnic background? The respondents' answer is coded as:

1= White

2= Black/African American

3= American Indian/Alaskan Native

4= Asian, Pacific Islander

5= Hispanic/Spanish

Only categories 1=whites; and 2= black/African American are used, and are recoded as a dummy variable such that (black/African American=0; whites=1)

### *Age*

Respondents' age is measured by asking the question: In what year were you born? I computed this variable by subtracting the respondents given year from the year 2004.

To capture the effect of age on fear of Cyber-Crime, and to be consistent with previous research on fear of crime age is recoded into three categories ( Ferraro, 1995; Rountree and Land, 1996; and Clemente, and Kleiman, 1977): 1) less than 25 yours-old; 2) 25-50 years-old; 3) older than 50 yours old. Then, it is dummy coded such that:

-Less than 25 years-old =1.

-25-50 years-old =1.

-Older than 50 yours old=0 (reference category).

### *Education*

The respondents' level of education is measured by asking the question: How many years of formal education have you completed? So, this variable is measured by year, which ranges from 0 to 25 years of formal education.

### *Income*

The respondent's income is measured by asking: What is your total 2003 household income before taxes. The respondents are asked to choose a category that best describes their income:

- 1) Less than \$10,000
- 2) 10 - \$20,000
- 3) 20 - \$40,000
- 4) 40 - \$60,000
- 5) 60 - \$80,000

- 6) 80 - \$100,000
- 7) More than \$100,000

Because of missing data that income variable has, I applied the following procedure to save such missing data:

- 1) I recoded income into three categories: 1) low income (categories 1 and 2); 2) mid income (categories 3 and 4); high income (categories 5, 6, and 7); 4)
- 2) I created a missing income category (includes missing data).
- 3) I dummy coded income such that:
  - Low income =1.
  - Mid income =1.
  - Missing incime =1
  - High income =0 (reference category).

#### *Rural-Urban Place of Residence*

This variable will be measured by asking respondents the question: Which of the following best describes your place of residence. The respondents will be asked to choose one that best describes their place of residence:

- 1. A farm or ranch
- 2. Rural but not on a farm
- 3. A town under 2,500 population
- 4. A town with 2,500 to 10,000 people
- 5. A city of 10,000 to 50,000



6. A city of 50,000 to 100,000, or

7. A city larger than 100,000

Rural-urban place of residence variable is recoded into two categories: rural, and urban. To classify a place of residence as urban or rural, I used Census Bureau classification. Census Bureau defines urban in the decennial census as “comprised of all territory people and housing units in incorporated places of 2500 or more.” (GARM, 1994, P 12-2). So, categories 1 to 3 is recoded as rural, and categories 4 to 7 is recoded as urban. Then, I dummy coded this variable such that (rural=1; urban=0).

### *Interaction Terms*

#### Age\*Gender

As discussed in the review of the literature, gender seems to work different with age. That is, there is an interaction effect between gender and age. The effect of gender on fear of crime is strong for young people, but diminishes with age (Liska et al, 1988). Warr (1984) found that the effect of the age-gender interaction on fear of crime was significant for ten offenses he examined. So, an interaction term of age and gender is created. Age\*gender is a product of multiplying two dummy age variables (<25 years old; and 25-50 years old) by the dummy gender variable. Therefore, two interaction variables were created. These variables are:

<25 years old \*gender.

25-50 years old\*gender.

### Gender\*Cyber-Crime Victimization

To further examine the effect of gender and Cyber-Crime victimization on fear of Cyber-Crime, I created an interaction term between gender and Cyber-Crime victimization. Here, I multiply the dummy gender variable by the dummy Cyber-Crime victimization variable.

### Plan of Analysis

As discussed in the literature, the Internet Crime Complaint Center (IC3) referred 190,143 complaints to enforcement agencies on behalf of individuals. These complaints included many different types of fraud such as auction fraud, non-delivery, and credit/debit card fraud, as well as non-fraudulent complaints, such as computer intrusions, spam/unsolicited e-mail, and child pornography. This is almost a 100 percent increase over 2003 when 95,064 complaints were referred. Also, in 2004 there has been an increase in almost every kind of security threat that affects computers. One hundred thousand barriers were broken by known viruses and the number of new viruses increased by more than 50 percent since 2003 (Ward, Mark Technology Correspondent, BBC News website, 2004). So, it will be very crucial for the proposed study to describe the nature and the prevalence of the Cyber-Crime victimization among U.S. adults living in households with Internet access. Therefore, a descriptive analysis of the prevalence and the nature of Cyber-Crime victimization is provided.

This study's aim is to investigate Cyber-Crime victimization among Internet users in the United States by: 1) assessing the factors that impact computer virus victimization;

2) assessing the factors that impact Cyber-Crime victimization; and 3) predicting fear of Cyber-Crime. Thus, three models are developed. The first predicts computer virus victimization, the second predicts Cyber-Crime victimization, and the third fear of Cyber-Crime.

As Figure 3 indicates, I predict computer virus victimization by frequency, duration, have children who have access to the Internet, and money-target variables. I expect that all these independent variables have a positive relationship with computer virus victimization controlling for age, gender, income, education, rural-urban, and race variables.

As Figure 4 indicates, I predict Cyber-Crime victimization by frequency, duration, have children who have access to the Internet, id-target, and money-target variables. I expect that all these independent variables have a positive relationship with Cyber-Crime victimization controlling for age, gender, income, education, rural-urban, and race variables.

In the third model, as figure 5 depicts, I will predict fear of Cyber-Crime by Cyber-Crime victimization, known victims, have children who have access to the Internet, gender (females), perceived seriousness, age\*gender and gender\*Cyber-Crime victimization. These independent variables are expected to have positive relationships with fear of Cyber-Crime controlling for age, race, education, and income variables.

Since the dependent variables, computer virus victimization and Cyber-Crime victimization are categorical variables, logistic regression is the appropriate statistical procedure. Logistic regression is a statistical technique that is widely used whenever a

dependent variable is a dichotomous. Computer virus victimization and Cyber-Crime victimization are dichotomous variables, which has binary responses (yes=1, and no=0). I developed four nested models to predict computer virus victimization, and five nested model to predict Cyber-Crime victimization.

In the fear of Cyber-Crime model, OLS multiple regression is used because the dependent variable, fear of Cyber-Crime, is measured as an ordinal-level variable. SPSS is used to run this model. To test fear of Cyber-Crime, I developed two nested models

I created a variety of measures using data reduction procedures. The measures include: Cyber-Crime victimization, fear of Cyber-Crime, id-target, and money-target. I present the following:

- Univariate statistics for relevant indicators
- Bivariate statistics for relevant indicators
- Logistic regression to predict computer virus victimization.
- Logistic regression to predict Cyber-Crime victimization
- OLS regression to predict Fear of Cyber-Crime.

**Control Variables**

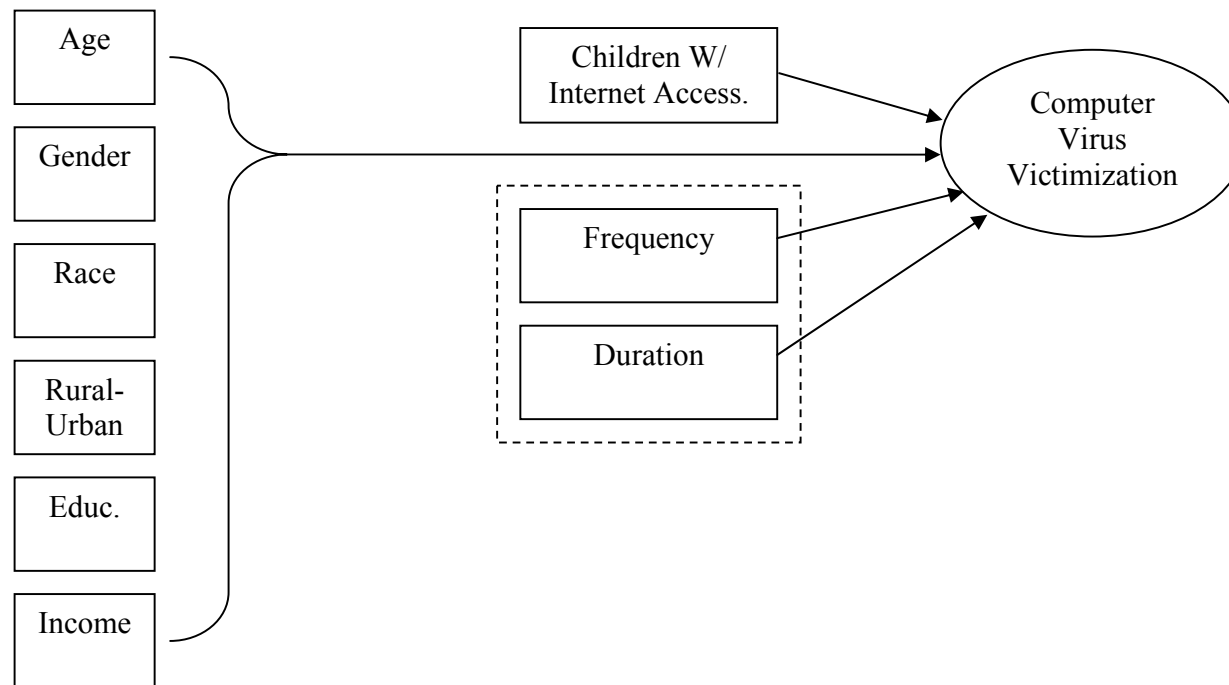


Figure 3. Computer Virus Victimization Model

**Control Variables**

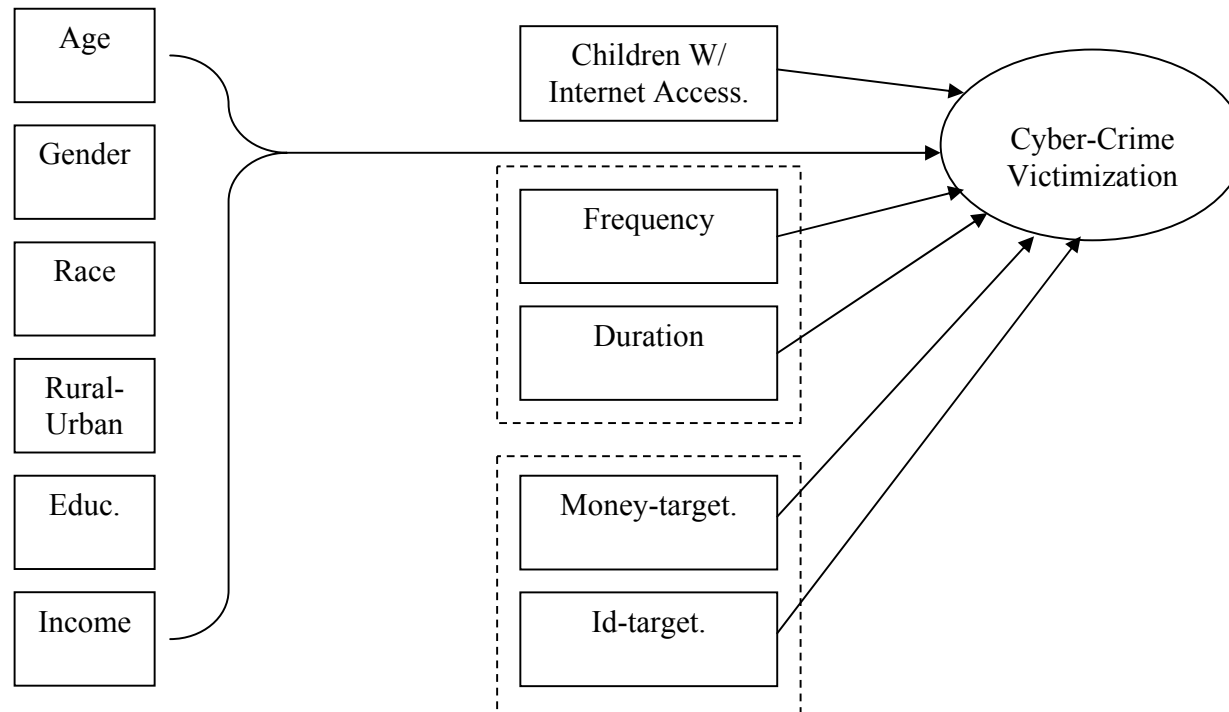


Figure 4. Cyber-Crime Victimization Model

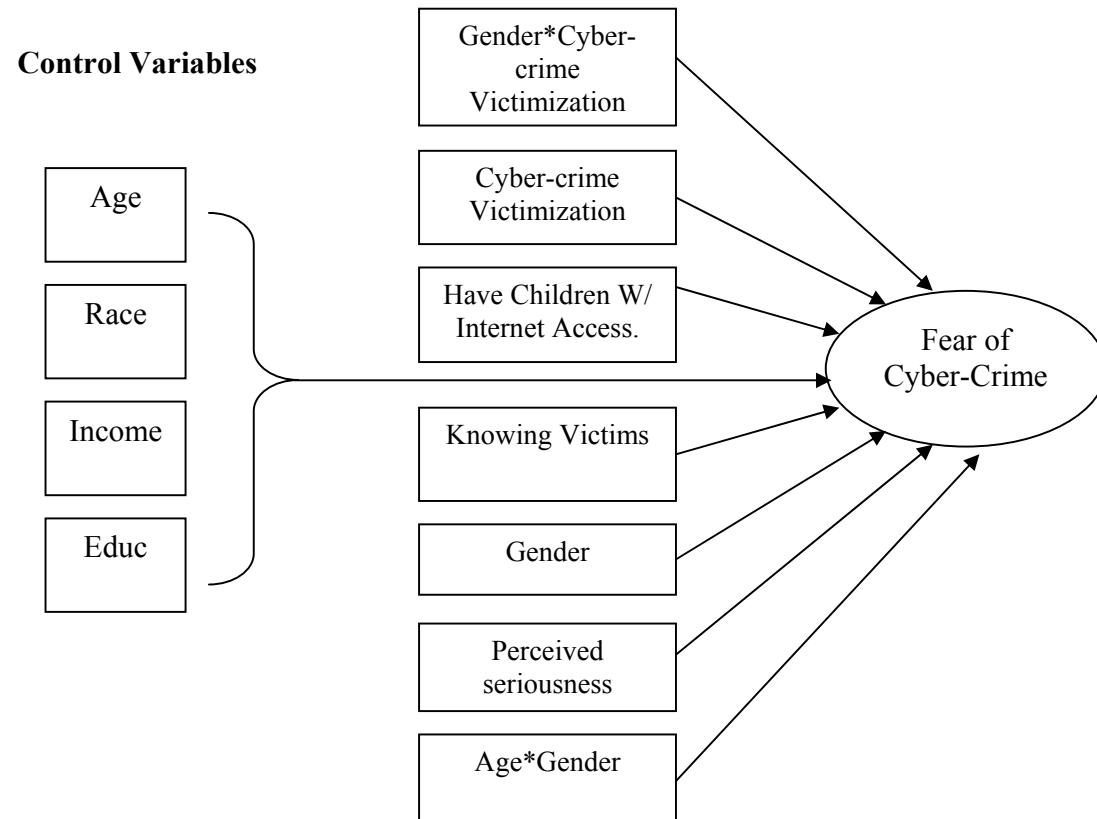


Figure 5. Fear of Cyber-Crime Model

### Study Limitation

Although the aim of this study is to investigate Cyber-Crime victimization among Internet users in the United States by using two approaches: routine activity and fear of crime, the data does not allow a comprehensive test of all the components of these two approaches.

As for the routine activity approach, the absence of guardianship element, which is considered to be one important element of the theory besides motivated offender, and suitable targets, cannot be tested in the current study. This variable, although it is in the 2004 National Cyber Crime Victimization Survey, cannot be used. In the process of conducting the survey a mistake happened. That is, instead of asking all respondents the question: “Do you use any anti-virus, anti-spam, or anti-spy software to protect your computer system? This question was asked to only those who have been victimized. Therefore, I cannot use this variable to measure the absence of guardianship. However, in Cyber-Crime victimization, I can assume that capable guardianship is absent when Cyber-Crime occurs. Guardianship, as mentioned above, is electronic guardians, ranges from firewalls, anti-virus and anti-spy software. These electronic guardians have to be installed and updated in computers by users in order to be effective. However, these electronic guardianships are not enough to fully protect computers from being hacked or attacked by virus.



ICSA Labs 8th Annual Computer Virus Prevalence Survey in 2002<sup>2</sup> shows that rates of virus and malware infection were increasing every month. However, 96% of the respondents said that they had 90% of their computers and 92% of their email servers protected with antivirus software and updated. The survey concluded that although the use of anti-virus software is important it is not enough.

Perceived risk in the fear of crime approach is considered to be one of the predictors of fear of crime, as the fear of crime literature suggests. Yet, perceived risk cannot be tested in this study because the data does not include such a measure.

---

<sup>2</sup> “ICSA Labs — a division of TruSecure Corporation — has independently collected vital statistics on the state of the computer virus problem and published its findings in its trusted Computer Virus Prevalence Survey since 1994. This report is considered the industry’s definitive study of viruses and their impact. Its findings are studied by industry analysts, media outlets, government agencies, global corporations and others to gain insight on the virus threat”.

(<http://www3.ca.com/Solutions/Collateral.asp?CID=41607&ID=156>)

## CHAPTER IV

### UNIVARIATE AND BIVARIATE STATISTICS

In this chapter several tables are presented to describe the independent variables and dependent variables of the study. Percentages are presented for gender, race, type of resident, income, children with access to the Internet, known victim, and victimization variables. Means and standard deviation are presented for frequency, duration, age, and education. Explanatory factor analysis and reliability test are presented for the variable fear of Cyber-Crime. As for bivariate statistics, the dependent variables (viruses, and Cyber-Crime victimization) are analyzed by gender, race, type of resident, income, and children with access to the Internet. Duration, frequency, money-target, id-target, and fear of Cyber-Crime are analyzed by gender, race, and communication via email.

#### Univariate Statistics

As table 4.1 indicates, 59.6 percent of the sample is female, and 94.6 percent is white. More than half of the respondents (64.5 percent) live in urban places. About half of the sample has an income over \$ 20,000 and less than \$80,000. About eighty five percent of the respondents have children with access to the Internet. Those who know one of their family members or friends who have been a victim of a computer-related crime constitute 10.4 percent of the sample.

Table 4.1 Frequencies and Percentages of Selected Variables

<b>Variables</b>	<b>N</b>	<b>%</b>
<b>Gender</b>		
<i>Males</i>	485	40.3
<i>Females</i>	719	59.6
<b>Race</b>		
<i>Whites</i>	1075	94.6
<i>Blacks</i>	61	5.4
<b>Place of Residence</b>		
<i>Rural</i>	360	31.6
<i>Urban</i>	779	64.5
<b>Children w/access to Internet?</b>		
<i>Yes</i>	846	85.1
<i>No</i>	135	13.6
<i>Don't Know/Not Sure</i>	13	1.3
<b>Income</b>		
<i>&lt; \$10,000</i>	20	1.7
<i>10 - \$20,000</i>	55	4.6
<i>20 - \$40,000</i>	191	15.8
<i>40 - \$60,000</i>	227	18.8
<i>60 - \$80,000</i>	176	14.6
<i>80-\$100,000</i>	104	8.6
<i>\$100,000 &gt;</i>	152	12.6
<b>Known Victims</b>		
<i>Has one of your family members or friends ever been the victim of a computer-related crime?</i>		
<i>Yes</i>	125	10.4
<i>No</i>	1022	84.7
<i>Don't Know/Not Sure</i>	59	4.9

Table 4.2 presents descriptive statistics of some variables of the study. The mean age of the sample is 48.39 with a standard deviation of 15.29. The mean formal education of the respondents is 14.98 years with a standard deviation of 2.48.

As table 4.2 shows, the mean of the frequency of using the Internet by the respondents is 4.59, which implies that the respondents use the Internet on average several days a week to once a day. The duration of staying online has a mean of 2.06, which means that respondents stay online a little more than one hour.

Table 4.2 Descriptive Statistics of Selected Variables

<b>Variables</b>	<b>Mean</b>	<b>SD</b>
Age	48.39	15.29
Year of Formal Education	14.98	2.48
Frequency <sup>a</sup>		
<i>On average, how often would you say you get on the Internet at home?</i>	4.55	1.26
Duration! <sup>b</sup>		
<i>When you use the Internet at home, how long do you usually stay online at one time?</i>	2.00	1.12

<sup>a</sup>0. Never; 1. A few times per year; 2. Once or twice a month; 3. Once or twice a week

4. Several days a week; 5. Once a day; 6. Several times each day

<sup>b</sup> 1. 30 minutes or less; 2. 1 hour; 3. 1-2 hours; 4. 2-3 hours; 5. 3 or more hours

Table 4.3 shows the frequencies and percentages of Cyber-Crime victimization. More than half of the sample (61.2 %) reported that they had received a computer virus over the Internet. As for the other types of Cyber-Crimes, 3.7 percent of the respondents have been victimized by identity theft, 2.5 percent of the respondents have been victims of identity fraud or scam, 0.7 percent of the respondents have been victims of computer hacking, 0.4 percent of the respondents have been victims of cyberstalking or cyberharassment, 0.4 percent of the respondents have been victims of extortion or blackmail, and only 0.1 percent of the respondents have been victims of securities fraud or stock manipulation.

Although the percentages of Cyber-Crime victimization-except virus- seem to be small they represent millions of Internet users. For example, assuming that the sample of the survey is representative, 3.7 percent of the respondents who have been victimized by identity theft represents about eight millions of Internet users<sup>1</sup>.

---

<sup>1</sup> According to the InternetWorldStats.com, 2005, there are 224,103,811 Internet users in the United States.

Table 4.3 Frequencies and Percentages of Cyber-Crime Victimization

Variables	N	%
Have you ever received a computer virus over the Internet?		
<i>Yes</i>	739	61.2
<i>No</i>	444	36.8
<i>Don't know/ Not Sure</i>	24	2
Have you ever been the victim of a computer-related fraud or crime?		
<i>Yes</i>	92	7.6
<i>No</i>	1099	91.1
<i>Don't know/ Not Sure</i>	16	1.3
Identity fraud or scam offering bogus goods or services for money.		
<i>Yes</i>	30	2.5
<i>No</i>	59	4.9
<i>Refused</i>	3	0.2
<i>Doesn't apply</i>	1115	92
Identity theft like theft of your debit/credit card or security number.		
<i>Yes</i>	45	3.7
<i>No</i>	44	3.6
<i>Refused</i>	3	0.2
<i>Doesn't apply</i>	1115	92.4
Securities fraud or stock manipulation.		
<i>Yes</i>	1	0.1
<i>No</i>	88	7.3
<i>Refused</i>	3	0.2
<i>Doesn't apply</i>	1115	92.4
Cyberstalking or cyberharassment.		
<i>Yes</i>	5	0.4
<i>No</i>	84	7.0
<i>Refused</i>	3	0.2
<i>Doesn't apply</i>	1115	92.4
Extortion or blackmail via the internet.		
<i>Yes</i>	4	0.4
<i>No</i>	85	7.0
<i>Refused</i>	3	0.2
<i>Doesn't apply</i>	1115	92.4
Computer hacking.		
<i>Yes</i>	8	0.7
<i>No</i>	81	6.7
<i>Refused</i>	3	0.2
<i>Doesn't apply</i>	1115	92.4

Table 4.4 Frequencies and Means of Fear of Cyber-Crime

Variables	Not at all concerned		Somewhat concerned		Very concerned		Mean
	(1)		(2)		(3)		
	N	Percent	N	Percent	N	Percent	
<i>That you might receive a virus that would damage your computer system.</i>	141	11.7	413	34.2	652	54	2.43
<i>That your computer might be accessed/hacked by other users.</i>	247	50.5	418	34.6	537	44.5	2.25
<i>About entering your debit or credit card numbers over the Internet.</i>	235	19.5	373	30.9	597	49.5	2.3
<i>That you might become a victim of a computer—related crime</i>	296	24.5	451	37.4	453	37.5	2.14

Table 4.4 shows the frequencies and means for the fear of Cyber-Crime measures. More than 80% of the sample (mean= 2.43) is somewhat to very concerned about getting viruses that would damage their computer system. About the same percentage of the sample is also somewhat to very concerned about entering debit or credit card numbers over the Internet. More than 70% of the sample is somewhat to very concerned that their computer might be accessed or hacked by others and that they might become victims of

computer-related crime. These items will be combined in a scale reflecting fear of Cyber-Crime.

### Factor Analysis

Factor analysis is a statistical procedure mainly used to reduce large numbers of variables that are intercorrelated into a small number of dimensions or factors (Nachmias & Nachmias, 1992). Furthermore, it is very useful in constructing scales. Factor analysis involves two steps: extraction and rotation. Extraction determines how many factors underlie a set of variables. One of the most common used methods of extraction is Principle Component. As a rule of thumb in deciding how many factors should be included, factors with an eigenvalue of 1.0 or more may be included.

Rotation makes the interpretation of factors easier. There are different methods of rotation, but the most common used is Varimax rotation. Varimax rotation is an orthogonal rotation. It makes the results clear and makes it possible to identify each variable with a single factor by maximizing the variance of the squared loadings of a factor on all the variables in a factor matrix.

As discussed in the literature, fear of crime has traditionally been measured by only a single indicator rather than multiple indicators. Such indicators do not allow for reliability tests to make sure that the measure of fear of crime is a valid measure. In this study I create a measure of fear of Cyber-Crime. This measure includes multiple indicators rather than a single indicator. Also, this measure will meet the criteria developed by Ferraro (1995) in that it refers to a specific crime, i.e., Cyber-Crime. It will



tap the state of worry about cyber crime, and it will directly assess Cyber-Crime victimization in the subject's everyday use of the Internet.

Table 4.5 Factor Analyses of Fear of Cyber-Crime Items

<b>Variables: How concerned are you...</b>	<b>Factor Loadings</b>
That you might receive a virus that would damage your computer system.	.795
That your computer might be accessed/ hacked by other users.	.844
About entering your debit or credit card numbers over the Internet.	.651
That you might become a victim of a computer-related crime.	.776
Eigenvalue= 2.370	
Reliability= .765	

As table 4.5 indicates, factor analysis results in one factor with an eigenvalue=2.370. The fear of Cyber-Crime items have high factor loadings, which means they reflect one underlying dimension, that is fear of Cyber-Crime. The reliability test of these items shows that these items have an Alpha score of .765.

## Bivariate Statistics

### *Cyber-Crime Victimization*

Tables 4.6.1 to 4.6.8 are cross tabulation of Cyber-Crimes by selected variables. These tables are intended to examine the distribution of Cyber-Crime across some demographic variables. As table 4.6.1 indicates, males (66.8%), and whites (62.3 %) have significantly higher computer virus victimization than females and blacks. Subjects who have children with Internet access have significantly higher computer virus victimization (62.3%) than those who do not have. However, whites, and those who have children with Internet access are overrepresented in the sample.

Other Cyber-Crime victimizations such as computer-related fraud, identity fraud or scam, identity theft, securities fraud, cyber-stalking, extortion or blackmail, and computer hacking are all higher among females. However, only identity fraud or scam victimization is significant at 0.05 level.

As for race, whites have higher Cyber-Crime victimization in all types of Cyber-Crime except extortion or blackmail, which is significantly higher among black. Although the chi-square for such difference is significant at 0.01 level, there are only three cases, so it is not possible to generalize in any meaningful way.

As table 4.6.1 shows, subjects who live in urban places have higher victimizations across all types of Cyber-Crimes. However, there are no statistically significant differences between urban and rural types of residence.

Subjects who have children with Internet access have higher victimization across all types of Cyber-Crime. But, only computer virus victimization, as mentioned above, registers a significant difference between those who have children with Internet access and those who do not.

Subjects who have lower income, less than \$ 20,000, exhibit lower Cyber-Crime victimization than those who have higher income. However, there are no statistically significant differences among these categories. Similar table examining the distribution of Cyber-Crime across age categories, income categories, frequency, and duration is provided in Appendix B.

Table 4.6.1 Cross-Tabulation of Cyber-Crime Victimization by Selected Variables

Variables	Computer virus		Computer-related fraud or crime		Identity fraud or scam		Identity theft		Securities fraud		Cyber-stalking		Extortion or blackmail		Computer hacking	
	N	%	N	%	N	%	N	%	N	%	N	%	N	%	N	%
Gender																
Male	324	66.8	31	34.1	14	48.3	15	33.3	0	0	1	20	0	0	3	37.5
Female	414	57.6	60	65.9	15	51.7	30	66.7	1	100	4	80	4	100	5	62.5
Chi-square	9.598***		1.438		3.873*		.024		.523		.468		2.167		.046	
Race																
Whites	670	62.3	86	96.6	28	96.6	44	100	1	100	5	100	1	33.3	8	100
Blacks	29	47.5	3	3.4	1	3.4	0	0	0	0	0	0	2	66.7	0	0
Chi-square	6.281**		.749		.000		3.256		.037		.192		36.853**		.319	
Place of Residence																
Rural	214	30.6	33	37.1	14	48.3	14	31.8	1	100	2	40	1	33	3	37.5
Urban	485	69.4	56	62.9	15	51.7	30	68.2	0	0	3	60	2	66.7	5	62.5
Chi-square	.414		1.394		2.294		1.121		1.707		.018		.020		.000	

\*Significance at p<.05

\*\*Significance at p< .01

\*\*\*Significance at p< .001

Table 4.6.1 (Continued)

Variables	Computer virus		Computer-related fraud or crime		Identity fraud or scam		Identity theft		Securities fraud		Cyber-stalking		Extortion or blackmail		Computer hacking	
	N	%	N	%	N	%	N	%	N	%	N	%	N	%	N	%
Children w/access to Internet?																
Yes	527	62.3	63	86.3	21	87.5	31	88.8	1	100	2	66.7	3	100	6	100
No	74	54.8	10	13.7	2	8.3	5	13.5	0	0	1	33.3	0	0	0	0
Chi-square	3.015*		.000		.253		.443		.131		1.486		.404		.847	
Income																
< \$10,000	11	1.9	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10 - \$20,000	26	4.6	6	8.2	1	4	3	8.1	0	0	0	0	1	33.3	0	0
20 - \$40,000	117	20.5	16	21.9	7	28	5	13.5	1	100	0	66.7	1	33.3	1	16.7
40 - \$60,000	142	24.9	13	17.8	3	12	9	24.3	0	0	0	0	1	33.3	3	50
60 - \$80,000	109	19.1	15	20.5	6	24	9	24.3	0	0	0	0	0	0	0	0
80-\$100,000	62	10.9	7	9.6	2	8	4	10.8	0	0	0	0	0	0	1	16.7
\$100,000 >	104	18.2	16	21.9	6	24	7	18.9	0	0	1	33.3	0	0	1	16.7
Chi-square	9.452		5.665		2.941		4.531		3.854		5.113		4.639		6.079	

\*Significance at p&lt;.05

\*\*Significance at p&lt; .01

\*\*\*Significance at p&lt; .001

Tables 4.6.2 to 4.6.8 compare mean education, age, frequency of use, and duration of use between those who have been victimized by Cyber-Crime and those who have not. As table 4.6.2 shows, those who have been victimized by computer virus have more years of formal education than those who have not. There are significant differences between those who have been victimized and those who have not regarding the frequency and duration of using the Internet. Subjects who are victimized use the Internet more frequently and stay longer on line. The mean age of the computer virus victims is less than non victims. However, there is no statistically significant difference between the two groups.

Table 4.6.2 Mean Comparisons of Selected Variables

Variables	Computer Virus?				Mean Difference
	Yes		No		
	Mean	SD	Mean	SD	
Years of formal education	15.15	2.58	14.65	2.25	0.50***
Age	47.71	14.28	49.44	16.8	1.74
Frequency <sup>a</sup>	4.71	1.158	4.29	1.37	0.415***
Duration <sup>b</sup>	2.1	1.14	1.83	1.06	0.273***

<sup>a</sup> 1. A few times per year; 2. Once or twice a month; 3. Once or twice a week 4. Several days a week; 5. Once a day; 6. Several times each day.

<sup>b</sup> 0. never ;1. 30 minutes or less; 2. 1 hour; 3.1-2 hours; 4. 2-3 hours; 5. 3 or more hours

\*\*\*Significance at  $p < .001$

As table 4.6.3 indicates, subjects who are victimized by identity fraud or scam and those who are not have almost the same amounts of formal education, the same age, use the Internet and stay on line at the same frequency and duration.

Table 4.6.3 Mean Comparisons of Selected Variables

Variables	Identity Fraud or Scam				Mean Difference
	Yes		No		
	Mean	SD	Mean	SD	
Years of formal education	15.83	3.15	15.49	2.6	0.34
Age	46.73	15.27	46.2	14.7	0.53
Frequency <sup>a</sup>	5.06	1.06	4.91	.987	0.157
Duration <sup>b</sup>	2.58	1.37	2.56	1.25	0.025

<sup>a</sup>1. A few times per year; 2. Once or twice a month; 3. Once or twice a week 4. Several days a week; 5. Once a day; 6. Several times each day.

<sup>b</sup>0. never ;1. 30 minutes or less; 2. 1 hour; 3.1-2 hours; 4. 2-3 hours; 5. 3 or more hours

Subjects who have been victimized by identity theft seem to be older, use the Internet less frequently, and stay on line for less time than those who have not, as table 4.6.4 shows. However, there are no statistically significant differences.

Table 4.6.4 Mean Comparisons of Selected Variables

Variables	Identity Theft				Mean Difference
	Yes		No		
	Mean	SD	Mean	SD	
Years of formal education	15.69	2.66	15.52	2.9	0.17
Age	47.688	15.24	45.05	14.45	2.64
Frequency <sup>a</sup>	4.86	1.01	5.07	1.01	0.206
Duration <sup>b</sup>	2.488	1.21	2.65	1.37	0.17

<sup>a</sup>1. A few times per year; 2. Once or twice a month; 3. Once or twice a week 4. Several days a week; 5. Once a day; 6. Several times each day.

<sup>b</sup>0. never ;1. 30 minutes or less; 2. 1 hour; 3.1-2 hours; 4. 2-3 hours; 5. 3 or more hours

As for computer-related fraud or crime, table 4.6.5 shows that victims have one year more of formal education than non-victims. Victims of computer-related fraud or crime use the Internet more frequent and stay longer on line than non victims. Also, the table shows that victims are almost two years younger than non-victims. However, there is no statistically significant difference between the two groups regarding age.

Table 4.6.5 Mean Comparisons of Selected Variables

Variables	Computer-Related Fraud or Crime				Mean Difference
	Yes		No		
	Mean	SD	Mean	SD	
Years of formal education	15.70	2.8	14.92	2.44	0.78**
Age	46.07	14.98	48.53	15.31	2.46
Frequency <sup>a</sup>	4.95	1.02	4.51	1.26	0.439***
Duration <sup>b</sup>	2.51	1.29	1.95	1.08	0.562***

<sup>a</sup> 1. A few times per year; 2. Once or twice a month; 3. Once or twice a week 4. Several days a week; 5. Once a day; 6. Several times each day.

<sup>b</sup> 0. never ;1. 30 minutes or less; 2. 1 hour; 3.1-2 hours; 4. 2-3 hours; 5. 3 or more hours

\*\*Significance at  $p < .01$

\*\*\*Significance at  $p < .001$

Table 4.6.6 indicates that cyber-stalking victims are younger than non-victims, have one year less of formal education than non victims, use the Internet a little less frequent than non-victims, but stay about the same time on line.



Table 4.6.6 Mean Comparisons of Selected Variables

Variables	Cyber-stalking				Mean Difference
	Yes		No		
	Mean	SD	Mean	SD	
Years of formal education	14	2.8	15.7	2.77	1.7
Age	40.6	16.9	46.7	14.7	6.12
Frequency <sup>a</sup>	4.8	.83	4.97	1.02	0.175
Duration <sup>b</sup>	2.6	.54	2.56	1.32	0.032

<sup>a</sup> 1. A few times per year; 2. Once or twice a month; 3. Once or twice a week 4. Several days a week; 5. Once a day; 6. Several times each day.

<sup>b</sup> 0. never ;1. 30 minutes or less; 2. 1 hour; 3.1-2 hours; 4. 2-3 hours; 5. 3 or more hours

Table 4.6.7 shows that victims of extortion or blackmail are younger, and have one year and half less of formal education than non-victims. But, victims use the Internet more frequently, and stay longer on line than non-victims. However, the only significant difference in mean between victims of extortion or blackmail and non-victims is duration.

Table 4.6.7 Mean Comparisons of Selected Variables

Variables	Extortion or Blackmail				Mean Difference
	Yes		No		
	Mean	SD	Mean	SD	
Years of formal education	14	2.16	15.68	2.8	1.68
Age	32.75	5.85	47.02	14.8	14.27
Frequency <sup>a</sup>	5	1	4.96	1.01	0.036
Duration <sup>b</sup>	4.66	.577	2.49	1.24	2.17**

<sup>a</sup> 1. A few times per year; 2. Once or twice a month; 3. Once or twice a week 4. Several days a week; 5. Once a day; 6. Several times each day.

<sup>b</sup> 0. never ;1. 30 minutes or less; 2. 1 hour; 3.1-2 hours; 4. 2-3 hours; 5. 3 or more hours

\*\*Significance at  $p < .01$

As for extortion or blackmail victimization, table 4.6.8 shows that victims and non-victims have almost the same years of formal education. But, victims are four years younger than non-victims, use the Internet more frequent and stay online a little longer than non-victims. However, there are no statistically significant differences between the two groups.

Table 4.6.8 Mean Comparisons of Selected Variables

Variables	Extortion or Blackmail				Mean Difference
	Yes		No		
	Mean	SD	Mean	SD	
Years of formal education	15.13	2.53	15.65	2.82	0.53
Age	42.12	15.48	46.80	14.8	4.67
Frequency <sup>a</sup>	5	1.19	4.96	1.01	0.038
Duration <sup>b</sup>	2.75	1.388	2.55	1.28	0.1987

<sup>a</sup> 1. A few times per year; 2. Once or twice a month; 3. Once or twice a week 4. Several days a week; 5. Once a day; 6. Several times each day.

<sup>b</sup> 0. never ;1. 30 minutes or less; 2. 1 hour; 3.1-2 hours; 4. 2-3 hours; 5. 3 or more hours

### *Fear of Cyber-Crime*

Tables 4.7, 4.8 and 4.9 compare the mean differences between males and females, whites and blacks, and rural and urban type of residence regarding fear of Cyber-Crime measure items.

As table 4.7 shows, females are more concerned than males about receiving a virus, having their computer accessed or hacked, entering their credit or debit number over the Internet, and becoming victims of computer-related crime. Although the mean

differences between males and females are not large, they are statistically significant at at least 0.01.

Table 4.7 Mean Comparisons of Fear of Cyber-Crime Items by Gender

Variables	Male		Female		Mean Difference
	Mean	SD	Mean	SD	
<i>That you might receive a virus that would damage your computer system.</i>	2.35	.711	2.47	.675	0.12**
<i>That your computer might be accessed/hacked by other users.</i>	2.17	.769	2.29	.778	0.12**
<i>About entering your debit or credit card numbers over the Internet.</i>	2.19	.803	2.37	.752	0.19***
<i>That you might become a victim of a computer—related crime</i>	2.04	.773	2.19	.778	0.15***

1. Not all concerned; 2. Somewhat concerned; 3. Very concerned  
 \*\*Significance at  $p < .01$ ; \*\*\* Significance at  $p < .001$

Table 4.8 shows that whites and blacks do not differ in their concerns about receiving a virus, having their computer accessed or hacked, entering their credit or debit number over the Internet, and becoming victims of computer-related crime. Both are somewhat to very concerned. There are no statistically significant differences between the two groups.

Table 4.8 Mean Comparisons of Fear of Cyber-Crime Items by Race

Variables	White		Black		Mean Difference
	Mean	SD	Mean	SD	
<i>That you might receive a virus that would damage your computer system.</i>	2.42	.688	2.41	.739	0.01
<i>That your computer might be accessed/hacked by other users.</i>	2.23	.773	2.28	.859	0.05
<i>About entering your debit or credit card numbers over the Internet.</i>	2.29	.769	2.38	.799	0.08
<i>That you might become a victim of a computer—related crime</i>	2.13	.772	2.11	.896	0.02

Also, table 4.9 shows that subjects who live in urban places and subjects who live in rural places exhibit the same concern about receiving a virus, having their computer accessed or hacked, entering their credit or debit number over the Internet, and becoming victims of computer-related crime. There are no statistically significant differences between the two groups.

Table 4.9 Mean Comparisons of Fear of Cyber-Crime Items by Type of Residence

Variables	Rural		Urban		Mean Difference
	Mean	SD	Mean	SD	
<i>That you might receive a virus that would damage your computer system.</i>	2.47	.671	2.40	.696	0.07
<i>That your computer might be accessed/hacked by other users.</i>	2.21	.798	2.25	.756	0.04
<i>About entering your debit or credit card numbers over the Internet.</i>	2.29	.821	2.31	.748	0.02
<i>That you might become a victim of a computer—related crime</i>	2.17	.797	2.11	.767	0.06

### *Internet Behavior*

Tables 4.10 and 4.11 are cross-tabulation of Internet activities by gender and race. As table 4.10 shows, there are differences between males and females in using the Internet. Internet activities such as rent a car, buying books, movies or music, paying bills, checking or making financial investments, advertising a car, researching a specific health-related issue, setting a web page, and looking for a job have higher frequencies among females than males. On the other hand, Internet activities such as researching a car for buying, buying a car, and taking a web-based class are practiced more by males than females. There are no statistically significant differences between males and females in the other Internet activities such as researching travel and/or lodging information, buying

airline tickets or hotel rooms, scheduling classes at a school, using an on-line auction site, and looking to hire someone.

Table 4.10 Cross-tabulation of Internet Activities by Gender

Variables	Males		Females		Chi-Square
	N	%	N	%	
Researched travel and/or lodging information.	398	87.8	578	85.8	0.537
Bought airline tickets or hotel rooms.	268	58.8	384	57.0	0.361
Rented a car.	162	35.5	176	26.1	11.497**
Bought books, movies or music.	261	57.2	347	51.5	3.622*
Bought or had flowers sent.	56	12.3	69	10.2	1.154
Paid bills.	129	28.3	141	20.9	8.123**
Checked or made financial investments.	179	39.3	221	32.8	4.971*
Researched cars you might buy.	183	40.1	182	27.0	21.438***
Advertised a car you wanted to sell.	311	68.2	408	60.5	6.91*
Bought a car.	52	11.4	36	5.3	13.92***
Taken a web-based class.	34	7.5	16	2.4	16.61***
Scheduled classes at a school.	62	13.6	93	13.8	0.01
Used an on-line auction site.	47	10.3	70	10.4	0.02
Research a specific health-related issue.	212	46.5	261	38.7	6.742*
Set up a web page.	307	67.3	513	76.1	10.55**
Looked for jobs/employment.	98	21.5	115	17.1	3.48*
Looked to hire someone.	171	37.5	239	35.5	0.490

Table 4.11 shows that whites and blacks differ in some of the Internet activities. Internet activities such as researching travel and/ or lodging information, researching a specific health-related issue, setting up a web page, and researching a specific health-related issue are practiced by whites more than blacks. The other Internet activities seem to be practiced by whites and blacks at the same frequencies.

Table 4.11 Cross-tabulation of Internet Activities by Race

Variables	Whites		Blacks		Chi-Square
	N	%	N	%	
Researched travel and/or lodging information.	877	87.0	45	77.6	4.163*
Bought airline tickets or hotel rooms.	580	57.5	34	58.6	0.026
Rented a car.	301	29.9	16	27.6	.0136
Bought books, movies or music.	545	54.1	28	48.3	0.740
Bought or had flowers sent.	112	11.1	6	10.3	0.033
Paid bills.	242	24.0	10	17.2	1.391
Checked or made financial investments.	349	34.6	24	41.4	1.10
Researched cars you might buy.	328	32.5	15	25.9	1.12
Advertised a car you wanted to sell.	642	63.7	37	63.8	.000
Bought a car.	74	7.3	7	12.1	1.746
Taken a web-based class.	42	4.2	3	5.2	0.137
Scheduled classes at a school.	137	13.6	8	13.8	0.002
Used an on-line auction site.	105	10.4	5	8.6	0.191
Research a specific health-related issue.	438	43.5	10	17.2	15.456***
Set up a web page.	736	73.0	35	60.3	4.34*
Looked for jobs/employment.	190	18.8	9	15.5	0.401
Looked to hire someone.	356	35.3	28	48.3	3.996*

Tables 4.12, 4.13, and 4.14 compare the mean differences between males and females, whites and blacks, rural and urban type of residence regarding the behavior of using the Internet. As table 4.12 shows, males use the Internet more frequent than females. But, there are no statistically significant differences about the duration of using the Internet between the two groups.

Table 4.12 Mean Comparisons of Selected Variables by Gender

Variables	Male		Female		Mean Difference
	Mean	SD	Mean	SD	
Frequency <sup>a</sup>	4.7	1.18	4.43	1.29	0.278***
Duration <sup>b</sup>	2.028	1.16	1.98	1.09	0.046

<sup>a</sup> 1. A few times per year; 2. Once or twice a month; 3. Once or twice a week 4. Several days a week; 5. Once a day; 6. Several times each day.

<sup>b</sup> 0. never ;1. 30 minutes or less; 2. 1 hour; 3.1-2 hours; 4. 2-3 hours; 5. 3 or more hours

\*\*\*Significance at  $p < .001$

\*\*Significance at  $p < .01$

Table 4.13 indicates that males use the Internet more frequent than blacks. But, blacks stay online more than whites.

Table 4.13 Mean Comparisons of Selected Variables by Race

Variables	White		Black		Mean Difference
	Mean	SD	Mean	SD	
Frequency <sup>a</sup>	4.56	1.25	4.089	1.4	0.48**
Duration <sup>b</sup>	1.95	1.08	2.36	1.31	0.41**

<sup>a</sup> 1. A few times per year; 2. Once or twice a month; 3. Once or twice a week 4. Several days a week; 5. Once a day; 6. Several times each day.

<sup>b</sup> 0. never ;1. 30 minutes or less; 2. 1 hour; 3.1-2 hours; 4. 2-3 hours; 5. 3 or more hours

\*\*Significance at  $p < .01$



As table 4.14 indicates, subjects who live in urban places use the Internet more frequent than those who live in rural places. However, both groups seem to be the same regarding how much time they stay on line.

Table 4.14 Mean Comparisons of Selected Variables by Type of Residence

Variables	Rural		Urban		Mean Difference
	Mean	SD	Mean	SD	
Frequency <sup>a</sup>	4.43	1.28	4.61	1.22	0.1857*
Duration <sup>b</sup>	1.99	1.12	2.00	1.11	0.102

<sup>a</sup> 1. A few times per year; 2. Once or twice a month; 3. Once or twice a week 4. Several days a week; 5. Once a day; 6. Several times each day.

<sup>b</sup> 0. never ;1. 30 minutes or less; 2. 1 hour; 3.1-2 hours; 4. 2-3 hours; 5. 3 or more hours

\*Significance at  $p < .05$

### *Correlation Matrix*

Table 4.15 shows the Pearson's correlation coefficients for the three dependent variables- computer virus victimization, Cyber-Crime victimization, and fear of Cyber-Crime- with control variables-age, gender, race, income, education, and type of residence- and independent variables-frequency, duration, children with access to the Internet, id-target, money-target, knowing victim, and perceived seriousness.

The correlation coefficients should be interpreted with caution because some of the variables are categorical variables (1=yes; 0=no). As table 4.15 shows, there are significant positive relationship between computer virus victimization and fear of Cyber-Crime (0.130), gender (male)(0.090), race (white)(0.070), frequency (.159), duration (0.117), id target (0.155), money-target (0.178), knowing victim (0.111). But, computer

virus victimization negatively correlates with education (-.099), and does not correlate with children with access to the Internet. The significant correlations between computer virus victimization and frequency and duration, as shown above, are consistent with what the study proposes.

Table 4.15 depicts significant and positive association between gender (male)(0.066), race (white)(0.07), education (0.101), frequency (0.177), duration (0.177), id-target (0.207), money-target (0.198), and knowing victim (0.177). Also, the table shows that there is a negatively significant association between Cyber-Crime victimization and age (-0.068). The correlations found between Cyber-Crime victimization and frequency, duration, id-target, and money-target are consistent with the hypotheses of the study.

Fear of Cyber-Crime, as table 4.15 indicates, significantly and positively correlates with Cyber-Crime victimization (0.141), gender (female)(0.122), and perceived seriousness (0.086). But, not statistically significant relationships were observed between fear of Cyber-Crime and age, race, income, children with access to the Internet, and knowing victim.

Also, table 4.15 depicts significant positive association between frequency and gender (male)(0.108), race (white)(0.083), and type of residence (urban)(0.069). Significant positive association was observed between duration and race (black)(0.082), and negative association between duration and income (0.0106).

Table 4.15. Correlation Matrix of All Variables

	Computer Virus	Cyber-crime	Fear of Cyber-crime	Age	Gander (Male)	Race (White)	Educ.	Type of Residence (Rural)	Income
<b>C. Virus†</b>	_____								
<b>Cyber-crime</b>	0.866**	_____							
<b>Fear of CC</b>	0.130**	0.141**	_____						
<b>Age</b>	-0.55	-0.068*	0.006	_____					
<b>Gander††</b>	0.090**	0.066*	-0.122**	-0.004	_____				
<b>Race††</b>	0.075*	0.070*	-0.008	-0.099**	-0.038	_____			
<b>Educ.</b>	-0.099**	0.101**	-0.041	-0.003	0.113**	0.046	_____		
<b>Type of Res.††</b>	-0.019	-0.001	-0.013	-0.020	-0.038	0.066*	-0.111**	_____	
<b>Income</b>	0.068	0.061	-0.035	-0.052	-0.109**	0.115**	0.282**	-0.107**	_____
<b>Freq.</b>	0.159**	0.177**	-0.009	0.005	0.108**	0.083**	0.096**	-0.069*	0.041
<b>Duration</b>	0.117**	0.177**	0.040	-0.100**	0.020	-0.082**	-0.017	-0.004	-0.106**
<b>Id-target</b>	0.155**	0.207**	0.007	-0.145**	0.052	-0.009	0.174**	-0.065*	0.209**
<b>Money-target</b>	0.178**	0.198**	-0.023	-0.081**	0.102**	0.010	0.226**	-0.103**	0.299**
<b>ChildrenW/IA†</b>	0.032	0.024	0.007	0.389**	0.075**	0.062*	0.025	0.016	0.075*
<b>Knowing Vctm†</b>	0.111**	0.177**	0.037	0.043	-0.019	0.030	0.078**	-0.022	0.029
<b>Seriousness†</b>	0.037	0.037	0.086**	-0.035	-0.052	-0.024	-0.055	-0.032	-0.009

Table 4.15 (Continued)

	<b>Freq.</b>	<b>Duration</b>	<b>Id-Target</b>	<b>Money-Target</b>	<b>Children w/ Internet Access</b>	<b>Knowing Victims</b>	<b>Perceived seriousness</b>
<b>Freq.</b>	—						
<b>Duration</b>	0.157**	—					
<b>Id-target</b>	0.233**	0.224**	—				
<b>Money-target</b>	0.219**	0.148**	0.572**	—			
<b>ChildrenW/IA†</b>	0.046	-0.022	0.057*	0.017	—		
<b>Knowing Vctm†</b>	-0.017	-0.062*	-0.127**	-0.061*	-0.033	—	
<b>Seriousness†</b>	-0.001	0.034	-0.014	-0.015	0.069*	-0.008	—

\*Significance at  $p < .05$ \*\*Significance at  $p < .01$ 

†These variables are binary variables (yes=1; no=0), where 1= victimized by computer virus; male; white; rural; children with access to the Internet; known victims; seriousness

†† These variables are measured on nominal level.

## CHAPTER V

### MULTIVARIATE ANALYSIS

In this chapter logistic regression models for the two dependent primary variables, (i.e., computer virus victimization, and Cyber-Crime victimization) and OLS regression models for fear of Cyber-Crime are presented. In logistic regression models, I apply routine activity approach to predict computer virus victimization, and Cyber-Crime victimization. As discussed in the literature, the Internet is a place that presents a high risk of victimization. High risk is reflected by frequency and duration of using the Internet. The suitable targets on the Internet that are valuable, attractive and at high risk of illegal use are personal information (i.e., id-target), and credit/ debit card numbers (i.e., money-target) that are stored on the Internet.

To test the effects of the routine activity variables and the other variable that I hypothesized (i.e., children with access to the Internet) I present three nested models for computer virus victimization, and four models for Cyber-Crime victimization. I entered these variables as a block starting with control variables in order to determine how much effect routine activity variables have in predicting victimization, and to reach the most parsimonious model.

So, the first model includes the control variables (age, gender, race, types of residence, income, and education). The second model includes the control variables and

children with access to the Internet. Frequency and duration are introduced into model three with the control variables and children with access to the Internet. A diagnostic of the logistic regression models is offered.

For Cyber-Crime victimization as a dependent variable, four models are presented. The first model includes the control variables (age, gender, race, types of residence, income, and education). The second model includes the control variables and children with access to the Internet. Frequency and duration are introduced into model three with the control variables and children with access to the Internet. The fourth model includes the control variables, children with access to the Internet, frequency, duration money-target, and id-target. A diagnosis of the logistic regression models is offered.

In OLS regression, I draw on the fear of crime literature to predict fear of Cyber-Crime. As discussed in the review of the literature, fear of crime is conditioned by the following variables: gender, age, race, SES, perceived risk, incivilities, and victimization. So, based on the hypotheses I developed, two models were presented to examine the effect of age, and race, education, and income as control variables, and gender, children with access to the Internet, Cyber-Crime victimization, knowing victims, and perceived seriousness, as independent variables, on fear of Cyber-Crime. So, the first model includes only the control variables, and the second model includes control variables and gender, children with access to the Internet, Cyber-Crime victimization, knowing victims, and perceived seriousness variables.

The rationale of including perceived seriousness as a predictor of fear of Cyber-Crime, as discussed in the methodology section, is that in of the literature of fear of crime perceived seriousness is implied given the nature of traditional crime. In Cyber-Crime, the effect of perceived seriousness is not known. So, it is essential to examine such effect.

### *Logistic Regression Diagnosis*

Logistic regression is a statistical technique that is widely used whenever a dependent variable is dichotomous. Computer virus victimization is a dichotomous variable, which has binary responses (yes=1, and no=0). To use logistic regression, a diagnostic procedure has to be done in order to make sure that the assumptions of the logistic regression are not violated. Violations of logistic regression assumptions could result in “biased coefficients, inefficient estimates or invalid statistical inferences” (Menard, 2002 P 67).

The logistic regression assumptions are no specification error, linearity relationship, and collinearity. Also, outlying cases have to be detected because they may exert influential effects which bias the parameter estimates in logistic regression.

Testing for specification error was carried out using STATA. The LinkTest procedure in STATA is used to test for specification error. Hatsq is found to be nonsignificant across all models, which means that the no specification error assumption is not violated.

Collinearly assumption is tested using SPSS. I used OLS regression for each model with collinearity diagnostics selected. Variance Inflation Factor (VIF) values were

all under 10, and Tolerance values were all far from zero. So, no multicollinearity is found across the models.

As for outlying cases, Menard (2002) suggests to use Studentized residual, the Leverage, and Dbeta. Four cases were found to be more than 3 in Studentized residual test. These outlying cases are 943, 972, 973, and 191. These outlying cases were influential because when they were deleted the model chi-square in model one, for example, improved from 37.520 to 40.038. Consequently, the sample size was reduced from 991 to 987 cases for all models.

The Dbeta test reveals that all cases across all independent variables were less than 1, which means that there were no outlying cases detected. As for the Leverage test, the expected value is:

$$Leverage = \frac{k+1}{N} = \frac{14+1}{991} = \frac{15}{991} = 0.0151$$

No cases were found to be several times this expected leverage value. All cases were found to range from 0.0044 to 0.05. So, there were no outlying cases in this test.

## Computer Virus Victimization Models

### *Model 1*

In model one, as table 5.1 shows, only control variables are included. For every one year increase in the age the odds of becoming a victim of computer virus decreases by 1.2 % holding all other variables constant in the model. This means that younger people are more likely to become victims of computer viruses.



Controlling for all other variables in the model, the odds of males getting a computer virus is 61.4 % higher than the odds of females. The odds of whites becoming victims of computer virus is 93.8 % higher than the odds of blacks when holding all other variables constant in the model. This means that whites are more likely to get a computer virus than blacks. When controlling for every other variables in the model, for every year increase in formal education the odds of becoming a victim of a computer virus increases by 9.1 %. Income and type of residence show no statistically significant effect on computer virus victimization.

The model chi-square (40.038) with degree of freedom (8) is significant at the 0.001 level. This indicates that the goodness of fit of the overall model is significant and it is better than a model with only an intercept.

### *Model 2*

As table 5.1 indicates, model two includes the control variables and children with access to the Internet. The effects of age, gender, and race on computer virus victimization increase in magnitude when children with access to the Internet is introduced to the model.

For every one year increase in age the odds of becoming a victim of a computer virus decrease by 1.6 % holding all other variables constant in the model. This means that when people get older the likelihood of becoming victim by computer virus decreases.

Controlling for all other variables in the model, the odds of males getting a computer virus is 65.5 % higher than the odds of females. The odds of whites becoming

victims of a computer virus is 95.6 % higher than the odds of blacks when holding all other variables constant in the model. This means that whites are more likely to get a computer virus than blacks. When controlling for every other variable in the model, for every year increase in formal education the odds of becoming a victim of a computer virus increases by 9 %.

Holding all other variables constant in the model, the odds of those who have children with access to the Internet getting computer viruses is 73.1 % higher than the odds of those who do not have. Income and type of residence show no statistically significant effect on computer virus victimization.

The model chi-square (46.491) with 10 degree of freedom is significant at the 0.001 level. This indicates that the goodness of fit of the overall model is significant. Model 2 is a good model comparing to model 1. The addition of children with access to the Internet variable is significant at the 0.05 level, and it has improved the model<sup>1</sup>.

### *Model 3*

As table 5.1 shows, model three includes the control variables, children with access to the Internet, frequency, and duration. The effects of age, gender, education, and children with access to the Internet on computer virus victimization has decreased in their magnitudes due to the inclusion of frequency and duration, though they are still statistically significant. But, the effect of race on computer virus victimization increases.

<sup>1</sup>( Model 1  $X^2=40.038$ ;  $df=8$  )-(Model 2  $X^2=46.491$ ;  $df=10$ )=  $X^2$  6.453;  $df=2$  ( $P<0.05$ )

For every one year increase in age, the odds of becoming a victim of a computer virus decreases by 1.4 % holding all other variables constant in the model. Controlling for all other variables in the model, the odds of males getting a computer virus is 60.2 % higher than the odds of females. The odds of whites becoming victims of computer virus is 99 % higher than the odds of blacks when holding all other variables constant in the model. This means that whites are more likely to get a computer virus than blacks.

When holding all other variables constant in the model, for every year increase in formal education the odds of becoming a victim of a computer virus increases by 8.6 %.

Holding all other variables constant in the model, the odds of those who have children with access to the Internet getting a computer virus is 64.2 % higher than the odds of those who do not have.

For every unit increase in the frequency of using the Internet, the odds of getting a computer virus increases by 18.2 % when holding all other variable constant in the model. For every hour increase in the duration of using the Internet, the odds of becoming a victim of a computer virus increases by 29 %. Income and type of residence show no statistically significant effects on computer virus victimization.

The model chi-square (73.097) with degree of freedom (12) is significant at the 0.001 level. This indicates that the goodness of fit of the overall model is significant. Also, model 3 is a good model comparing to model 2 and 1. The addition of frequency and duration variables is significant at the 0.001 level, and improved the model<sup>2</sup>.

<sup>2</sup>(Model 2  $X^2=46.491$ ;  $df=10$ )-(Model 3  $X^2 73.097$ ;  $df=12$  )= $X^2 26.606$ ;  $df=2$  ( $P<0.001$ )

To further explore the effects of the independent variables on computer virus victimization, I created interaction effects for gender and frequency, gender and duration, race and frequency, race and duration, and type of residence and frequency, and included them in the computer virus victimization models. But, they fail to achieve statistically significant effects except for race\*duration interaction term (see Tables 2.a through 2.c in Appendix C). However, blacks were underrepresented in the sample.

Table 5.1. Logistic Regression of Computer Virus Victimization  
(Dependent Variable: 1 =Yes)

Variables	Model 1		Model 2		Model 3	
	Coeffi	Wald	Coeffi	Wald	Coeffi	Wald
Age	-0.012* (0.988)	6.360	-0.016** (0.984)	10.407	-0.014** (0.986)	7.799
Gender <sup>1</sup>	0.479*** (1.614)	44.473	0.504*** (1.655)	12.499	0.472** (1.602)	10.60
Race <sup>2</sup>	0.662* (1.938)	4.999	0.671* (1.956)	5.096	0.688* (1.990)	5.143
Type of Residence <sup>3</sup>	-0.69 (0.934)	0.210	-0.070 (0.933)	0.226	-0.040 (0.961)	0.072
Education	0.087** (1.091)	8.592	0.086** (1.090)	8.220	0.083** (1.086)	7.332
Low Income <sup>4</sup>	-0.458 (0.632)	2.178	-0.412 (0.662)	1.733	-0.523 (.0592)	2.686
Mid Income	-0.010 (0.991)	0.003	0.001 (1.001)	.000	0.053 (0.949)	0.100
Income (missing)	0.119 (1.126)	0.389	0.132 (1.142)	0.481	0.179 (1.196)	0.854

Table 5.1. (Continued)

Variables	Model 1		Model 2		Model 3	
	Coeffi	Wald	Coeffi	Wald	Coeffi	Wald
Children w/access to Internet <sup>5</sup>			0.549* (1.731)	6.022	0.496* (1.642)	4.756
Children w/ access to Internet (missing)			0.293 (1.340)	1.291	0.235 (1.265)	0.801
Frequency					0.167** (1.182)	8.387
Duration					0.255*** (1.290)	13.039
Model X <sup>2</sup>	40.038***		46.491***		73.097***	
df	8		10		12	
n	987		987		987	

\*P<.05; \*\* P<.01; \*\*\*P<.001

Note: Numbers in parentheses are Exp(B)

1)female is the reference; 2) black is the reference; 3)urban is the reference; 4) high income is the reference;

5) children with no access to the Internet

## Cyber-Crime Victimization Models

As mentioned above, four models are presented to test the effect of the explanatory variables on Cyber-Crime victimization. Cyber-Crime victimization includes the following:

1. Computer virus
2. Internet fraud or scam offering bogus goods or services for money
3. Identity theft like theft of your debit/credit card or social security number
4. Securities fraud or stock manipulation
5. Cyberstalking or cyberharassment (via email for example)
6. Extortion or blackmail via Internet
7. Computer hacking (computer damage by amateur hackers)

### *Model 1*

In model one, as table 5.2 shows, only control variables are included. For every one year increase in the age the odds of becoming a victim of Cyber-Crime decreases by 1 % holding all other variables constant in the model. This means that younger people are more likely to become victims of computer virus.

Controlling for all other variables in the model, the odds of males becoming victims of Cyber-Crime is 62.1 % higher than the odds of females. The odds of whites becoming victims of Cyber-Crime is 91.7 % higher than the odds of blacks when holding all other variables constant in the model. This means that whites are more likely to be victims of Cyber-Crime than blacks. When controlling for every other variables in the

model, for every one year increase in formal education the odds of becoming a victim of Cyber-Crime increases by 8.6 %. Income and type of residence show no statistically significant effect on computer virus victimization.

The model chi-square (39.207) with 8 degree of freedom is significant at the 0.001 level. This indicates that the goodness of fit of the overall model is significant and it is better than a model with only an intercept.

### *Model 2*

As table 5.2 indicates, model two includes the control variables and children with access to the Internet. The effects of age, gender, and race on Cyber-Crime victimization increases in their magnitudes when children with access to the Internet was introduced to the model.

For every one year increase in the age the odds of becoming a victim of Cyber-Crime decreases by 1.5 % holding all other variables constant in the model. This means that when people get older the likelihood of becoming victim of Cyber-Crime decreases.

Controlling for all other variables in the model, the odds of males becoming victims of Cyber-Crime is 66.1 % higher than the odds of females. The odds of whites becoming victims of Cyber-Crime is 93.5 % higher than the odds of blacks when holding all other variables constant in the model. This means that whites are more likely to be victims of Cyber-Crime than blacks. When controlling for every other variables in the model, for every one year increase in formal education the odds of becoming a victim of Cyber-Crime increases by 8.4 %.



Holding all other variables constant in the model, the odds of those who have children with access to the Internet becoming victims of Cyber-Crime is 73.9 % higher than the odds of those who do not have. Income and type of residence show no statistically significant effect on computer virus victimization.

The model chi-square (45.552) with 10 degree of freedom is significant at the 0.001 level. This indicates that the goodness of fit of the overall model is significant. Model 2 is a good model comparing to model 1. The addition of children with access to the Internet variable is significant at the 0.05 level, and it has improved the model<sup>3</sup>.

### *Model 3*

As table 5.1 shows, model three includes the control variables, children with access to the Internet, frequency, and duration. The effects of age, gender, education, and children with access to the Internet on Cyber-Crime victimization has declined in their magnitude due to the inclusion of frequency and duration, though they are still statistically significant and in the same direction. But, the effect of race on Cyber-Crime victimization increases.

For every one year increase in age the odds of becoming a victim of Cyber-Crime decreases by 1.3 % holding all other variables constant in the model. Controlling for all other variables in the model, the odds of males becoming victims of Cyber-Crime is 60 % higher than the odds of females. The odds of whites becoming victims of Cyber-Crime is

<sup>3</sup>( Model 1  $X^2=39.207$ ;  $df=8$  )-(Model 2  $X^2=45.552$ ;  $df=10$ )=  $X^2 6.345$ ;  $df=2$  ( $P<0.05$ )

94.8 % higher than the odds of blacks when holding all other variables constant in the model. This means that whites are more likely to be victims of Cyber-Crime than blacks.

When holding all other variables constant in the model, for every one year increase in formal education the odds of becoming a victim of Cyber-Crime increases by 8 %. Holding all other variables constant in the model, the odds of those who have children with access to the Internet becoming victims of Cyber-Crime virus is 64.6 % higher than the odds of those who do not have.

For every time increase in the frequency of using the Internet, the odds of becoming a victim of Cyber-Crime increases by 21.6 % when holding all other variable constant in the model. For every one hour increase in the duration of using the Internet, the odds of becoming a victim of Cyber-Crime increases by 29.5 %. Income and type of residence show no statistically significant effect on computer virus victimization.

The model chi-square (75.516) with degree of freedom (12) is significant at least at 0.001 level. This indicates that the goodness of fit of the overall model is significant. Also, model 3 is a good model comparing to models 2 and 1. The addition of frequency and duration variables is significant at the 0.001 level, and it has improved the model<sup>4</sup>.

#### *Model 4*

Table 5.2 indicates that model 4 includes the control variables, children with access to the Internet, frequency, duration, money-target and id-target. The coefficients of age, education, children with access to the Internet become not statistically significant

<sup>4</sup>(Model 2  $X^2=45.552$ ;  $df=10$ )- (Model 3  $X^2 75.516$ ;  $df=12$  )= $X^2 29.964$ ;  $df=2$  ( $P<0.001$ )

due to the inclusion of money-target and id-target. The effects of gender and race on Cyber-Crime victimization increased a little comparing to model 3. The effects of frequency and duration decreased but were still statistically significant.

Controlling for all other variables in the model, the odds of males becoming victims of Cyber-Crime is 61.5 % higher than the odds of females. The likelihood of whites becoming victims of Cyber-Crime is 2.020 times higher than blacks when holding all other variables constant in the model.

For every one unit increase in the frequency of using the Internet, the odds of becoming a victim of Cyber-Crime increases by 14.3 % when holding all other variable constant in the model. For every one unit increases in the duration of using the Internet, the odds of becoming a victim of Cyber-Crime increases by 23.2 %.

For every increase in the number of times one divulges his/her credit or debit card number over the Internet, the odds of becoming a victim of Cyber-Crime increases by 19.8 % after controlling for all other variables in the model. Income and type of residence show no statistically significant effect on computer virus victimization. For every increase in the number of times one divulges his/her personal or id number, the odds of becoming a victim of Cyber-Crime increases by 13.4 % after controlling for all other variables in the model.

The model chi-square (100.031) with degree of freedom (14) is significant at the 0.001 level. This indicates that the goodness of fit of the overall model is significant.

Model 4 is a good model comparing to all other models with the addition of money-target and id-target variables is significant at the 0.001 level, and it has improved the model<sup>5</sup>

To further explore the effects of the independent variables on Cyber-Crime victimization, I created interaction effects for gender and frequency, gender and duration, race and frequency, race and duration, and type of residence and frequency, and included them in the Cyber-Crime victimization models. But, they fail to achieve statistically significant effects except for race\*duration interaction term (see Tables 1.a through 1.c in Appendix C). However, blacks were underrepresented in the sample.

---

<sup>5</sup> (Model 3  $X^2$  75.516; df=12)-(Model 4  $X^2$  100.031; df=14 )=  $X^2$  24.515; df=2 (P< 0.001)

Table 5.2. Logistic Regression of Cyber-Crime Victimization (Computer Virus and Other Types of Cyber-Crime)

(Dependent Variable: 1 = Yes)								
Variables	Model 1		Model 2		Model 3		Model 4	
	Coeffi	Wald	Coeffi	Wald	Coeffi	Wald	Coeffi	Wald
Age	-0.010*	4.741	-0.015**	8.369	-0.013*	6.019	0.009	2.703
	(0.990)		(0.985)		(0.987)		(0.991)	
Gender <sup>1</sup>	0.483**	11.316	0.508***	12.298	0.470**	10.176	0.480**	10.307
	(1.621)		(1.661)		(1.600)		(1.615)	
Race <sup>2</sup>	0.651*	4.826	0.660*	4.922	0.667*	4.789	0.703*	5.140
	(1.917)		(1.935)		(1.948)		(2.020)	
Type of Residence <sup>3</sup>	-0.051	0.117	-0.051	0.116	-0.016	0.011	0.037	0.058
	(0.951)		(0.950)		(0.984)		(1.038)	
Education	0.082**	7.451	0.081**	1.109	0.077*	6.142	0.054	2.831
	(1.086)		(1.084)		(1.080)		(1.055)	
Low Income <sup>4</sup>	-0.553	3.161	-0.510	2.646	-0.626	3.805	-0.392	1.416
	(0.575)		(0.601)		(0.535)		(0.676)	
Mid Income	-0.138	0.695	-0.129	0.60	-0.191	1.266	-0.026	0.022
	(0.871)		(0.879)		(0.826)		(0.974)	
Income (missing)	-0.010	0.003	0.002	0.000082	0.050	0.064	0.220	1.190
	(0.990)		(1.002)		(1.051)		(1.247)	

Table 5.2 (Continued)

Variables	Model 1		Model 2		Model 3		Model 4	
	Coeffi	Wald	Coeffi	Wald	Coeffi	Wald	Coeffi	Wald
Children w/access to Internet <sup>5</sup>			0.553*	6.039	0.498*	4.721	0.411	3.097
			(1.739)		(1.646)		(1.509)	
Children w/ access to Internet (missing)			0.309	1.417	0.249	0.882	0.189	0.493
			(1.362)		(1.283)		(1.208)	
Frequency					0.196**	11.307	0.133*	4.949
					(1.216)		(1.143)	
Duration					0.258***	12.825	0.209**	8.082
					(1.295)		(1.232)	
Money-target							0.181**	8.596
							(1.198)	
Id-target							0.126*	4.412
							(1.134)	
Model X <sup>2</sup>	39.207***		45.552***		75.516***		100.031***	
df	8		10		12		14	
n	987		987		987		987	

\*P&lt;.05; \*\* P&lt;.01; \*\*\*P&lt;.001

Note: Numbers in parentheses are Exp(B)

1) female is the reference; 2) black is the reference; 3) urban is the reference; 4) high income is the reference;

5) children with no access to the Internet

## Fear of Cyber-Crime Models

### *OLS Regression Diagnosis*

When using OLS regression, diagnosis procedures have to be carried out to make sure that regression assumptions are not violated. The regression assumptions are linearity, normality, constant variance, and independence. Violations of these assumptions could result in poor fit of the model.

As for linearity, theory and hypotheses suggest that all independent variables included in the models have linear relationship with the dependent variable, fear of Cyber-Crime. That is, fear of crime, as discussed in the literature, is predicted by: gender, age, race, SES, perceived risk, incivilities, and victimization. The dependent variable does not violate the normality assumption of OLS regression.

An analysis of the residuals reveals that no heteroscedasticity was detected when the studentized residual was regressed on a predicted variable. Two outlying cases were detected when residual analysis was carried out. Studentized residual analysis showed that these two outlying cases were close to 3. Deleting these outliers improve the coefficients of the models. So, the sample size was reduced from 987 to 985 cases.

### *Model 1*

In this model only control variables, age, race, education, and income are included. As table 5.3 shows, the mean score of fear of Cyber-Crime is lower by 0.284 units for younger people, who are in the age category of less than 25 years-old, than older

people, who are older than 50 years-old controlling for all other variables in the model. No statistically significant effects of race, education and income variables on fear of Cyber-Crime. The goodness of fit of the over all model is not good. The F-statistic (1.791) is not significant at the 0.05 level.

### *Model 2*

Model 2 includes the control variables and gender, children with access to the Internet, Cyber-Crime victimization, knowing victims, and perceived seriousness, as independent variables.

As table 5.3 indicates, the mean score of fear of Cyber-Crime is lower by 0.346 units for younger people, who are in the age category of less than 25 years-old, than older people, who are older than 50 years-old controlling for all other variables in the model. The mean score of fear of Cyber-Crime is 0.250 units higher for females than males, controlling for all other variables in the model.

The mean score of fear of Cyber-Crime is 0.265 units higher for those who have been victimized by Cyber-Crime than those who have not controlling for all other variables. The mean score of fear of Cyber-Crime is 0.148 units higher for those who feel that Cyber-Crime is a serious crime than those who don't, when holding all other variables constant. age category of 25-50 years-old, race, education, income, children with access to the Internet, and knowing victim have no statistically significant effects on fear of Cyber-Crime.



Based on F-statistic (3.879), which is significant at the .001 level, the overall model is good. The all variables in the model explain 4.9% of the variance in fear of Cyber-Crime. The inclusion of the independent variables has improved the model.

Table 5.3 OLS Regression of Fear of Cyber-Crime

Variables	Model 1		Model 2	
	b	t	b	t
Age <sup>1</sup>				
<25 years-old	-0.284*	-2.017	-0.346*	2.369
25-50 years-old	0.024	0.366	-0.042	0.624
Race <sup>2</sup>	-0.054	-0.376	-0.101	-0.718
Education	-0.018	-1.361	-0.019	1.417
Low Income <sup>3</sup>	0.168	1.116	0.143	0.961
Mid Income	0.073	0.964	0.057	0.762
Income (missing)	0.214*	2.415	0.183*	2.097
Gender <sup>4</sup>			0.250***	3.839
Children w/access to Internet <sup>5</sup>			-0.149	1.433
Children w/ access to Internet (missing)			-0.030	0.246
Cyber-Crime Victimization <sup>6</sup>			0.265***	3.911
Knowing Victim <sup>7</sup>			0.088	0.856
Perceived eriousness <sup>8</sup>			0.148*	2.109
R <sup>2</sup>	0.013		0.049	
F-Statistic	1.791		3.879***	
df	7		13	
N	985		985	

\*P<.05; \*\* P<.01; \*\*\*P<.001

Reference categories: 1) >50 years-old; 2) Black; 3) high income; 4) Male;

5) Children with no access to the Internet; 6) Not victimized;

7) No known victim; 8) No seriousness

To further explore the effects of the independent variables on fear of Cyber-Crime, I created three interaction terms of age and gender, as models three and four in table 5.4 show.

### *Model 3*

Model 3 includes the control variables and gender, children with access to the Internet, Cyber-Crime victimization, knowing victims, perceived seriousness, an interaction effect of <25 years-old \*gender, and an interaction effect of 25-50 years old\* gender as independent variables.

As table 5.4 indicates, the mean score of fear of Cyber-Crime is lower by 0.644 units for younger people, who are in the age category of less than 25 years-old, than older people, who are older than 50 years-old controlling for all other variables in the model. The mean score of fear of Cyber-Crime is 0.257 units higher for females than males, controlling for all other variables in the model.

The mean score of fear of Cyber-Crime is 0.268 units higher for those who have been victimized by Cyber-Crime than those who have not controlling for all other variables. The mean score of fear of Cyber-Crime is 0.150 units higher for those who feel that Cyber-Crime is a serious crime than those who don't, when holding all other variables constant. The mean score of fear of Cyber-Crime is 0.546 units higher for females who are less than 25 years-old than males when controlling for all other variables in the models.

Age category of 25-50 years-old, race, education, income, children with access to the Internet, knowing victim, and 25-50 years-old \*Gender have no statistically significant effects on fear of Cyber-Crime.

Based on F-statistic (3.536), which is significant at the .001 level, the overall model is good. The all variables in the model explain 5.4 % of the variance in fear of Cyber-Crime. The inclusion of the interaction variables has improved the model.

#### *Model 4*

Model 4 includes the control variables and gender, children with access to the Internet, Cyber-Crime victimization, knowing victims, perceived seriousness, and an interaction effect of gender\*Cyber-Crime victimization as independent variables.

As table 5.4 indicates, the mean score of fear of Cyber-Crime is lower by 0.341 units for younger people, who are in the age category of less than 25 years-old, than older people, who are older than 50 years-old controlling for all other variables in the model. The mean score of fear of Cyber-Crime is 0.149 units higher for those who feel that Cyber-Crime is a serious crime than those who don't, when holding all other variables constant. The mean score of fear of Cyber-Crime is 0.310 units higher for females who have been victimized by Cyber-Crime than those who have not when controlling for all other variables in the models. In other words, the effect of Cyber-Crime victimization on fear of Cyber-Crime differs by gender. Age category of 25-50 years-old, race, education, income, children with access to the Internet, knowing victim, gender, and Cyber-Crime victimization have no statistically significant effects on fear of Cyber-Crime.

Based on F-statistic (3.787), which is significant at the .001 level, the overall model is good. The all variables in the model explain 5.4 % of the variance in fear of Cyber-Crime.

Table 5.4. OLS Regression of Fear of Cyber-Crime (Interaction Terms)

Variables	Model 3		Model 4	
	b	t	b	t
Age <sup>1</sup>				
<25 years-old	-0.644**	-3.039	-0.341*	-2.337
25-50 years-old	0.007	0.067	-0.042	-0.621
Race <sup>2</sup>	-0.133	-0.939	-0.101	-0.621
Education	-0.019	-1.420	-0.019	-1.392
Low Income <sup>3</sup>	0.132	0.883	0.143	0.963
Mid Income	0.062	0.828	0.060	0.798
Income (missing)	0.178*	2.042	0.190*	2.177
Gender <sup>4</sup>	0.257**	2.768	0.037	0.319
Children w/access to Internet <sup>5</sup>	-0.146	-1.404	-0.140	-1.346
Children w/ access to Internet (missing)	-0.023	-0.189	-0.029	-0.232
Cyber-Crime Victimization <sup>6</sup>	0.268***	3.959	0.068	0.618
Knowing Victim <sup>7</sup>	0.101	0.982	0.089	0.867
Perceived Seriousness <sup>8</sup>	0.150*	2.129	0.149*	2.116
<25 years-old *Gender	0.546*	1.971		
25-50 years-old *Gender	-0.083	-0.636		
Gender*Cyber-Crime Victimization			0.310*	2.258
R <sup>2</sup>	0.054		0.054	
F-Statistic	3.536***		3.787***	
df	15		14	
N	985		985	

\*P&lt;.05; \*\* P&lt;.01; \*\*\*P&lt;.001

Reference categories: 1) &gt;50 years-old; 2) Black; 3) high income; 4) Male;

5) Children with no access to the Internet; 6) Not victimized;

7) No known victim; 8) No seriousness

## Summary of The Major Findings

### *Computer Virus Victimization Models*

1. When people get older the likelihood of being victims of a computer virus decreases.
2. Males are more likely than females to be victims of a computer virus.
3. Whites have a higher likelihood than blacks to be victims of a computer virus.
4. More educated people are more likely to be victims of a computer virus.
5. People who have children with access to the Internet are more likely to be victims of a computer virus.
6. The more frequently people use the Internet, the more likely they are to become victims of a computer virus.
7. People who stay longer on the Internet tend to have higher a greater likelihood of becoming victims of a computer virus.
8. Neither income nor type of residence have any effects on computer virus victimization.

### *Cyber-Crime Victimization Models*

1. Males are more likely than females to become victims of Cyber-Crime.
2. Whites are more likely to be victims of Cyber-Crime than blacks.
3. The more frequently people use the Internet, the more likely they will become victims of Cyber-Crime

4. People who stay longer on the Internet tend to have a greater risk of becoming victims of Cyber-Crime.
5. The more people divulge their credit or debit card number, the more they are at risk of becoming victims of Cyber-Crime.
6. The more people divulge their id or personal information, the more they are at risk of becoming victims of Cyber-Crime.
7. The effects of age, education, and children with access to the Internet on Cyber-Crime victimization are wiped out because of the inclusion of money-target and id-target (routine activity variables).
8. Neither income nor type of residence have they any effects on Cyber-Crime victimization

#### *Fear of Cyber-Crime Models*

1. Older people have higher levels of fear of Cyber-Crime than younger people.
2. Females have higher levels of fear of Cyber-Crime than males.
3. Females who are younger have higher levels of fear of Cyber-Crime than older.
4. Females who have been victimized by Cyber-Crime have higher levels of fear of Cyber-Crime than those who have not.
5. Those who have been victimized by Cyber-Crime fear more of Cyber-Crime than those who have not.
6. Those who think that Cyber-Crime is serious crime have higher level of fear of Cyber-Crime than those who do not.



7. Whites and blacks have the same level of fear of Cyber-Crime
8. Those who have children with access to the Internet and those who have not exhibit the same level of fear of Cyber-Crime.
9. Knowing victims of Cyber-Crime does not affect the fear of Cyber-Crime when controlling on other variables.

## CHAPTER VI

### DISCUSSION AND CONCLUSION

In this chapter I discuss the empirical findings of the study. Univariate, bivariate, and multivariate analysis (logistic regression and OLS regression) were utilized to investigate the extent to which research findings are consistent with hypotheses. The primary objective of this study was to investigate Cyber-Crime victimization among Internet users in the United States by: 1) assessing the factors that impact the victimization of computer virus; 2) assessing the factors that impact the victimization of Cyber-Crime; and 3) predicting fear of Cyber-Crime. Accomplishing this objective will further our criminological understanding of the new phenomenon of Cyber-Crime.

Ten hypotheses were tested. These hypotheses are presented in Table 6.1 with information regarding support or non-support of each hypothesis based on routine activity theory and fear of crime models. Based on the objective of the study, the organization of this chapter will be as follows: 1) discussion of the findings of computer virus victimization models; 2) discussing the findings of Cyber-Crime victimization; and 3) discussion of the findings of fear of Cyber-Crime. Then, I will discuss future research on the Cyber-Crime phenomena, and policy implications.

Table 6.1. Hypotheses and Support of Findings

Hypotheses	Supported	Routine Activity Theory	Fear of Cyber-crime
<i>H1</i> : It is expected that the more frequently one accesses the Internet the more likely he or she will be victimized, controlling for other relevant predictors.	Yes	X	
<i>H2</i> : It is expected that the longer one stays online the more likely he or she will be victimized.	Yes	X	
<i>H3</i> : It is expected that respondents whose children use the Internet will have a higher risk of victimization.	Partially	X	
<i>H4</i> : It is expected that activities on the Internet that involve divulging personal information will increase victimization.	Yes	X	
<i>H5</i> : It is expected that activities on the Internet that involve divulging personal financial information (i.e., credit card) will increase victimization.	Yes	X	
<i>H6</i> : Those who know someone who has been victimized will have higher levels of fear of cyber crime.	No		X
<i>H7</i> : It is expected that females will exhibit higher levels of fear of cyber-crime than males.	Yes		X
<i>H8</i> : It is expected that respondents whose children use the Internet will have higher levels of fear of cyber-crime.	No		X

Table 6.1. (continued)

Hypotheses	Supported	Routine Activity Theory	Fear of Cyber-crime
<i>H9</i> : It is expected that those who think that cyber-crime is a serious crime exhibit higher level of fear of cyber-crime than whites.	Yes		X
<i>H10</i> : Those who have experienced prior cyber-crime victimization will have higher levels of fear of cyber crime, controlling for other relevant predictors.	Yes		X

### *Computer Virus Victimization*

Computer virus is one type of Cyber-Crime. It is considered to be one of the new opportunities for traditional crime (Wall, 2005). The prevalence of computer virus victimization is high. A virus is a program or code that replicates itself onto other files with which it contacts. A virus can do harmful things to an infected computer by wiping out databases or files, damaging some important parts in a computer such as Bios, or forwarding a pornographic message to everyone listed in the email address book of an infected computer (Burden et al, 2003).

About 61.2% of the sample reported that they received a computer virus over the Internet (see table 4.3). When we look at the distribution of computer virus victimization, we see that males, whites, those who have children with access to the Internet, and those with more years of formal education have a higher likelihood of victimization than their counterparts (see table 4.6.1, and 4.6.2).

So, what impacts computer virus victimization? I tested three hypotheses for computer virus victimization. All of them were supported, as table 6.1 shows. The first hypothesis was that *it is expected that the more frequently one accesses the Internet the more likely he or she will be victimized, controlling for other relevant predictors*. The second hypothesis was that *it is expected that the longer one stays online the more likely he or she will be victimized*. These two hypotheses address risk exposure to computer virus victimization. As routine activity theory suggests, exposure to certain places at certain times increases victimization risk (Cohen and Felson 1979). The victimization literature has shown that risk victimization increases when people spend more time in

public places. Cohen et al (1981) defines exposure as “the physical visibility and accessibility of persons or objects to potential offenders at any given time or place” (p 507). In Cyber-Crime victimization, frequency and duration of Internet use determines the amount of time spent on the Internet, which is believed to be a high risk place. When a computer virus is created and distributed by a criminal over the Internet, any computer that is connected to the Internet is exposed. As model 3 in table 5.1 shows, the more frequently one uses the internet and longer one stays on the internet, the more likely he or she will be victimized by a computer virus. The elements of routine activity theory that are necessary for a crime converge. The suitable target here is a computer itself that is exposed. The absence of a capable guardian (i.e., anti-virus software) is assumed because the electronic guardians (anti-virus software) cannot fully protect computers from being infected by a virus.

Having children with access to the Internet increases the likelihood of being victimized by computer virus, as model 2 in table 5.1 shows. Two possible explanations are offered here. One, is that children may not be aware of potential threats that some websites have. So, they may download a file that contains a virus. Thus, computers became infected. The other explanation, which is supported by routine activity theory, is that when respondents of the survey reported that they have children with access to the Internet, they mean that they and their children use the Internet. This means that the frequency and duration of using the Internet increase, and, thus, their computers are at higher risk of exposure.

Findings from computer virus victimization models also show that younger people are more likely to be victims of a computer virus than older people, and males are more likely than females to be victims of a computer virus. These findings are consistent with the victimization literature. Males use the Internet more frequently than females, as table 4.12 shows. This means that males are more exposed to computer virus victimization than females. Unlike traditional victimization findings, however, whites have a higher likelihood than blacks to be victims of a computer virus. As table 4.13 shows, whites use the Internet more frequently than blacks. However, blacks in the survey are underrepresented, and this finding is substantially insignificant.

Another finding regarding computer virus victimization is that more educated people are more likely to be victims of a computer virus. The possible explanation for this finding is that educated people use the Internet more frequently. Younger people, males, whites, and more educated persons who have different computer activities and uses make them at higher risk to become victims of a computer virus.

The three variables, frequency, duration, and having children with access to the Internet, have powerful effects on computer virus victimization even after control variables were included.

Table 6.2 is the most parsimonious model, which includes only the variables that have significant effects on computer virus victimization. For every one year increase in age, the odds of becoming a victim of a computer virus decreases by 1.2 % holding all other variables constant in the model. Controlling for all other variables in the model, the odds of males getting a computer virus is 58 % higher than the odds for females. These

two findings are consistent with the traditional victimization literature. That is, younger persons and males are more likely to be victimized than older persons and females. It could be that they use the Internet more frequently, and, hence, are more exposed to victimization. The likelihood of whites getting a computer virus is 2.054 times higher than blacks when holding all other variables constant in the model. This means that whites are more likely to get a computer virus than blacks. This finding is contrary to the victimization literature. However, since blacks were underrepresented in the survey, I cannot count on this finding.

When holding all other variables constant in the model, for every year increase in formal education the odds of becoming a victim of a computer virus increases by 6.6 %. The possible explanation for this finding is that educated people may use the Internet more frequently.

Holding all other variables constant in the model, the odds of those who have children with access to the Internet getting a computer virus is 58.3 % higher than the odds of those who do not have children with access to the Internet. For every unit increase in the frequency of using the Internet, the odds of getting a computer virus increase by 12.7 % when holding all other variable constant in the model. For every hour increase in the duration of using the Internet, the odds of becoming a victim of a computer virus increases by 23.8 %.

The model chi-square (86.650) with degree of freedom (9) is significant at the 0.001 level. This indicates that the goodness of fit of the overall model is significant. Also, this model is a good model compared to all the previous models.



Controlling for age, gender, race, and education, the routine activity theory variables have robust effect on computer virus victimization, as table 6.2 shows.

Table 6.2. Logistic Regression of Computer Virus Victimization  
(Dependent Variable: 1 =Yes)

Variables	Coeffi	Wald
Age	-0.012* (0.988)	5.298
Gender <sup>1</sup>	0.457** (1.580)	9.896
Race <sup>2</sup>	0.720* (2.054)	5.579
Education	0.064* (1.066)	4.471
Children w/access to Internet <sup>3</sup>	0.459* (1.583)	4.028
Children w/ access to Internet (missing)	0.183 (1.200)	0.480
Frequency	0.120* (1.127)	4.189
Duration	0.213** (1.238)	9.221
Model X <sup>2</sup>	86.650	
df	9	
n	987	

\*P<.05; \*\* P<.01; \*\*\*P<.001

Note: Numbers in parentheses are Exp(B)

1) female is the reference; 2) black is the reference; 3) children with no access to the Internet

### *Cyber-Crime Victimization*

One aim of the study is to assess the factors that impact the victimization of Cyber-Crime. Cyber-Crime is defined as "crimes that are mediated by networked computers and not just related to computers" (Wall, 2005 P 79). Cyber-Crime is measured by whether or not a respondent was a victim of a Cyber-Crime. Cyber-Crime includes computer virus, Internet fraud or scam, identity theft, Securities fraud or stock manipulation, cyber-stalking or cyber-harassment, extortion or blackmail via Internet, and computer hacking.

The prevalence of Cyber-Crime is that more than half of the sample (61.2 %) reported that they had received a computer virus over the Internet, 3.7 percent of the respondents have been victimized by identity theft, 2.5 percent of the respondents have been victims of identity fraud or scam, 0.7 percent of the respondents have been victims of computer hacking, 0.4 percent of the respondents have been victims of cyberstalking or cyberharassment, 0.4 percent of the respondents have been victims of extortion or blackmail, and only 0.1 percent of the respondents have been victims of securities fraud or stock manipulation (see table 4.3).

Although the percentages of Cyber-Crime victimization-except virus- seem to be small they represent millions of Internet users. For example, assuming that the sample of the survey is representative, 3.7 percent of the respondents who have been victimized by identity theft represent about eight million Internet users<sup>1</sup>.

<sup>1</sup> According to the InternetWorldStats.com, 2005, there are 224,103,811 Internet users in the United States.

When we compare Cyber-Crime victimization, as shown above, to traditional crime victimization from 2002-2003 we see that Cyber-Crime victimization is more prevalent and is increasing. For example, for the total population 12 years old and older the estimated percentage of robbery is 0.159 percent, burglary is 1.29 percent, aggravated assault is 0.436 percent, and rape is 0.033 percent (Bureau of Justice Statistics: National Crime Victimization Survey, 2004). In addition, according to the Bureau of Justice Statistics (BJS) the nation's violent crime rate fell 10 percent in 2001, continuing a decline since 1994. Violent victimization and property crime rates in 2001 are the lowest recorded since the National Crime Victimization Survey's inception in 1973. For instance, the personal theft rate fell 33%; and the property crime rate fell 6%, from 178 to 167 victimizations per 1,000 households from 2000 to 2001 (BJS, 2002).

On the other hand, the number of victims of Cyber-Crime is on rise, given the increase in the number of Internet users. In 2004, the Internet Crime Complaint Center (IC3) referred 190,143 complaints to enforcement agencies on behalf of individuals. These complaints included many different types of fraud such as auction fraud, non-delivery, and credit/debit card fraud, as well as non-fraudulent complaints, such as computer intrusions, spam/unsolicited e-mail, and child pornography. This is almost a 100 percent increase over 2003 when 95,064 complaints were referred. The total dollar loss from all referred cases of fraud was \$68.14 million with a median dollar loss of \$219.56 per complaint. This indicates that Cyber-Crime victimization is more likely to occur than traditional street crime. So, what impacts Cyber-Crime victimization?

Five hypotheses were tested. All the hypotheses are supported except hypothesis 3, which is *It is expected that respondents whose children use the Internet will have a higher risk of victimization*. The other hypotheses that were supported are: *it is expected that the more frequently one accesses the Internet the more likely he or she will be victimized, controlling for other relevant predictors; it is expected that the longer one stays online the more likely he or she will be victimized; it is expected that activities on the Internet that involve divulging personal information will increase victimization; it is expected that activities on the Internet that involve divulging financial information (i.e., credit card) will increase victimization* (see table 6.1).

Using logistic regression, I found that the more frequently people use the Internet, the more likely they will become victims of Cyber-Crime; people who stay longer on the Internet tend to have a greater risk of becoming victims of Cyber-Crime; the more people divulge their credit or debit card number, the more they are at risk of becoming victims of Cyber-Crime; and the more people divulge their id or personal information, the more they are at risk of becoming victims of Cyber-Crime.

Frequency and duration measure risk exposure to Cyber-Crime victimization. As routine activity theory suggests, exposure to certain places at certain times increases victimization risk (Cohen and Felson 1979). The victimization literature has shown that risk increases when people spend more time in public places. Cohen et al (1981) define exposure as “the physical visibility and accessibility of persons or objects to potential offenders at any given time or place” (p 507). In Cyber-Crime victimization, frequency

and duration of Internet use determines the amount of time spent on the Internet, which is believed to be a high risk place.

Activities on the Internet that involve divulging personal information (id-target), and financial information (money-target) reflect suitable targets. As proposed by the routine activity theory, a victim may be absent from the sight of the crime (Felson and Clarke 1998). In Cyber-Crime victimization, therefore, those whose identity information and credit or debit card numbers are electronically stored on the Internet are always absent or have no control over them. Identity information and credit/debit numbers are the suitable targets and the absence of the possessor makes them easy targets. So, as shown on model 4 in table 5.2, id-target and money target have positive and significant effects on Cyber-Crime victimization.

Having children with access to the Internet increases the likelihood of being victimized by Cyber-Crime, as model 2 and 3 in table 5.2 shows. The two possible explanations for this finding are the same offered in computer virus victimization. But, when id-target and money-target are included in model 4, the effect of having children with access to the Internet became insignificant. The possible explanation is that children do not typically carry out financial transactions, such as buying or selling or any Internet activities that involve personal information, so they do not present id or money targets.

Those people who use the Internet more frequently, stay online longer, and engage in Internet activities that involve divulging their id information or financial information are more likely to be victims of Cyber-Crime. According to the routine activity theory, the three elements, motivated offender, suitable target, and the absence of

capable guardian have to converge in space and time. In cyber-space, how do they converge? In Cyber-Crime victimization, a space is cyberspace, which is reflected in websites, and chat rooms (Yar, 2005). Time in cyberspace has different implication than non-virtual world. Motivated offender and the victim do not have to be present in cyberspace at the same time in order for a crime to occur. An offender in cyberspace who creates a virus, for example, sends it over the Internet to many Internet users. Then, the virus waits for Internet users to log on the Internet. Once they log on, they are exposed to the threat of getting the virus. For example, the Chernobyl virus, which was released in 2000, affected many computers that were connected to the Internet, and damaged the Bios of the computers. Only those who logged on the Internet at that time were victimized.

What about the capable guardian, anti-virus software? As discussed in the literature review and methodology, anti-virus software cannot fully protect a computer from being infected by a virus. When a new virus is released, anti-virus software cannot recognize the new virus, until the anti-virus software developers (Symantec, and McAfee, for example) send an update to those who have such a software. Meanwhile, computers are not fully protected. So, those who frequently log on the Internet and stay longer are more likely to be exposed to Cyber-Crime.

In the case of the other types of Cyber-Crime, such as Internet fraud or scam, or identity theft, personal information and credit/debit card numbers are electronically stored on the Internet. Once Internet users enter their id numbers or credit/debit card numbers when they, for example, sell or buy goods, they are out of their control. A

hacker can send a Trojan horse over the Internet in order to hack a computer (Schell and Dodge, 2002). Once the Trojan horse is downloaded by the Internet user, his or her computer is under control of the hacker. A hacker, then, can steal any data from the victim's computer and monitors the victim's computer when the victim logs on the Internet.

Findings from Cyber-Crime victimization models also show that males are more likely than females to become victims of Cyber-Crime. These findings are consistent with the victimization literature. Males use the Internet more frequently than females, as table 4.12 shows. This means that males are more exposed to Cyber-Crime victimization than females. Unlike the traditional victimization literature, however, whites have a higher likelihood than blacks to be victims of Cyber-Crime. Since blacks in the survey are underrepresented, so this finding is substantially not significant.

Table 5.2 indicates that age, education, and children with access to the Internet lose statistical significance due to the inclusion of money-target and id-target. The effects of gender and race on Cyber-Crime victimization increased a little comparing to model 3. The effects of frequency and duration decreased but were still statistically significant. So, I ran another model, the most parsimonious model, as table 6.3 shows, which includes only the variables that have significant effects on Cyber-Crime victimization.

Controlling for all other variables in the model, the odds of males becoming victims of Cyber-Crime is 61.2 % higher than the odds of females. The likelihood of whites becoming victims of Cyber-Crime is 2.089 times higher than blacks when holding all other variables constant in the model.

For every one unit increase in the frequency of using the Internet, the likelihood of becoming a victim of Cyber-Crime increases by 14.1 % when holding all other variable constant in the model. For every one unit increase in the duration of using the Internet, the likelihood of becoming a victim of Cyber-Crime increases by 21 %.

For every increase in the number of times one divulges his/her credit or debit card number over the Internet, the odds of becoming a victim of Cyber-Crime increases by 22.6 % after controlling for all other variables in the model. For every increase in the number of times one divulges his/her personal or id number, the odds of becoming a victim of Cyber-Crime increases by 15.6 % after controlling for all other variables in the model.

The model chi-square (87.878) with degree of freedom (6) is significant at the 0.001 level. This indicates that the goodness of fit of the overall model is significant.

Controlling for gender and race, the routine activity theory variables have robust effect on Cyber-Crime victimization.



Table 6.3 Logistic Regression of Cyber-Crime Victimization  
(Dependent Variable: 1=Yes)

Variables	Coeffi	Wald
Gender <sup>1</sup>	0.477** (1.612)	10.560
Race <sup>2</sup>	0.737* (2.089)	5.766
Frequency	0.132* (1.141)	5.017
Duration	0.190** (1.210)	7.069
Money-target	0.204** (1.226)	11.612
Id-target	0.145* (1.156)	6.210
Model X <sup>2</sup>	87.878***	
df	6	
n	987	

\*P<.05; \*\* P<.01; \*\*\*P<.001

Note: Numbers in parentheses are Exp(B)

1) female is the reference; 2) black is the reference

### *Fear of Cyber-Crime*

Another objective of the current study was predicting fear of Cyber-Crime. With an increasing number of Internet users, increasing rate of Cyber-Crimes, and increasing

vulnerability of computer systems, victims of Internet crime are expected to increase.

Will this lead to increasing fear of Cyber-Crime?

Fear of crime has become an important research topic since the 1960s (Liska et al, 1982; Hale, 1996). To investigate this topic, I developed five hypotheses: 1) those who know someone who has been victimized will have higher levels of fear of cyber crime; 2) it is expected that females will exhibit higher levels of fear of Cyber-Crime than males; 3) it is expected that respondents whose children use the Internet will have higher levels of fear of Cyber-Crime; 4) as fear of crime literature suggests, it is expected that those who think that Cyber-Crime is a serious crime exhibit higher level of fear of Cyber-Crime than those who do not; 5) those who have experienced prior Cyber-Crime victimization will have higher levels of fear of cyber crime, controlling for other relevant predictors. Only three of these hypotheses were supported, as table 6.1 shows.

Fear of Cyber-Crime were measured by the following questions:

”How concerned are you.....”

- That you might receive a virus that would damage your computer system.
- That your computer might be accessed/hacked by other users.
- About entering your debit or credit card numbers over the Internet.
- That you might become a victim of a computer—related crime.

Respondents expressed their answers on a three-point Likert scale:

(1) Not at all concerned; (2) Somewhat concerned; (3) Very concerned. A single composite measure was created consisting of all the four items with an eigenvalue of

2.370 (Cronbach's  $\alpha=0.765$ ). Using factor analysis, these items are saved as a regression variable.

The fear of Cyber-Crime measure has an advantage over traditional fear of crime measures in the literature. The fear of Cyber-Crime measure includes multiple indicators rather than a single indicator. Also, this measure meets the criteria developed by Ferraro (1995) in that it refers to a specific crime ( i.e., Cyber-Crime) it taps the state of worry about cyber crime, and it directly assesses Cyber-Crime victimization in the subject's everyday using of the Internet.

Borrowing from fear of crime literature, the study found that: females have higher levels of fear of Cyber-Crime than males; those who have been victimized by Cyber-Crime fear more of Cyber-Crime than those who have not; and those who think that Cyber-Crime is serious crime have higher level of fear of Cyber-Crime than those who do not.

Females, particularly younger females, show more fear of Cyber-Crime than males. This finding is consistent with the fear of crime literature (Warr, 1984; Ferraro, 1995; Liska et al, 1988). Females are less likely to be victimized by Cyber-Crime, as discussed in the Cyber-Crime victimization. So, why are females fearful of crime? The fear of crime literature suggests that fear of rape among women "overshadows" other fear of other crimes (Ferraro, 1995). That is, women associate "nonsexual" crime with sexual crime. War (1984) suggests that there is "generality" of fear among women. But, there is a "core" fear among women, which is fear of sexual assault. Does the explanation offered by fear of crime literature hold true for fear of Cyber-Crime? The Cyber-Crimes

included in the measure of fear of Cyber-Crime are nonsexual crimes. Because females have generality of fear, it could be that they somehow associate Cyber-Crime with sexual crime. Getting a virus or being hacked increase the fear that their personal information and identity might be stolen, and, hence, they might be stalked or harassed.

Being victimized increases the fear of Cyber-Crime. In the fear of crime literature victimization as a predictor of fear of crime has generated conflicting results. Some researchers suggest that those who have been victimized are more fearful of crime (Smith and Hill, 1991). While some researchers find a weak relationship (Garofalo, 1979; Liska et al, 1988), other researchers find no relationship between victimization and fear of crime (Hill et al, 1985). Carl Keane (1995) claims that the victimization-fear of crime relationship exists when it involves certain offenses and offenders. The sample he used was from the Canadian Violence Against Women Survey. The findings of the current study are consistent with some of the fear of crime literature.

Being victimized by Cyber-Crime may cause negative consequences for victims, which has an impact on fear of Cyber-Crime. Being a victim of any type of Cyber-Crime has, as Smith and Hill (1991) claim, a “sensitizing effect”. Also, victimization works as a reminder of vulnerability (Keane, 1995). Victimization, then, increases one’s fear of Cyber-Crime.

The effect of victimization on fear of Cyber-Crime differs by gender, as model 4 in table 5.3 shows. That is, females who are victimized by Cyber-Crime have higher levels of fear of Cyber-Crime than males. As discussed above, females have generality of fear and it could be that they somehow associate Cyber-Crime with sexual crime even

though they are less likely to be victimized. But, when they are victimized they might reinforce the generality of fear

Perceived seriousness of crime shows an effect on fear of Cyber-Crime. Since perceived seriousness of Cyber-Crime has never been estimated in the literature, I provided a tentative measure and included it in the equation of fear of Cyber-Crime. Recall that perceived seriousness is measured by the survey question: “Persons convicted of committing computer-related crimes are not punished as severely as they should be”. (1= agree; 0= disagree).

Those who feel that Cyber-Crime is a serious crime exhibit a higher level of fear. This finding is consistent with the fear of crime literature. Contrary to Warr and Stafford’s (1983) claim that perceived seriousness would work better when it is combined with perceived risk, the measure of perceived seriousness of Cyber-Crime, used here, shows a significant independent effect on fear of Cyber-Crime. In other words, it could predict fear of Cyber-Crime. This measure of perceived seriousness of Cyber-Crime helps us understand how people perceive Cyber-Crime. If Cyber-Crime is perceived as a serious crime, then people associate it with traditional crime, which they fear.

Contrary to what was hypothesized, knowing someone who was victimized by Cyber-Crime did not have any effect on fear of Cyber-Crime. However, the fear of crime literature shows a mixed results regarding indirect victimization. Here, I found no support for indirect victimization. The reason for that could be that knowing someone who was victimized did not reinforce one’s sense of vulnerability to victimization. People

may think that they are better than others in terms of protection they have in their computers.

Another finding that is contrary to what was hypothesized is that those who have children with access to the Internet did not exhibit any effect on fear of Cyber-Crime. Borrowing from the fear of crime literature, I applied the concept altruistic fear from the work of Warr and Ellison (2000). The idea is that fear that people have for others in their lives (altruistic) is more common and intense than personal fear. So, people with children who have access to the Internet should be fearful about their children being victimized. However, this variable shows no effect on fear of Cyber-Crime. One explanation is that the dependent variable, fear of Cyber-Crime, does not include any item or question asking about the safety of one's children (Warr and Ellison, 2000). Fear of Cyber-Crime measure includes only questions about personal safety.

Findings from the fear of Cyber-Crime analysis show that older people have higher levels of fear of Cyber-Crime than younger people. The effect of age on fear of crime is not consistent across studies. As discussed in the review of the literature, some find that age has a positive relationship with fear of crime (Warr, 1984). Others find that age has a negative relationship with fear of crime (Rountree and Land, 1996). Yet, other studies find no significant effect of age on fear of crime (Ortega and Myles, 1987; Liska et al, 1988). Such discrepancy could result from using different measures of fear of crime. Studies that find a positive relationship between age and fear of crime use global measure of fear, whereas studies that use crime specific-fear find a negative relationship.

The current study finding that older people have higher levels of fear of Cyber-Crime contradicts what the literature of fear of crime suggests. I used specific-fear, which is fear of Cyber-Crime. However, I found positive relationship between age and fear. So, why, in the current study, are older people more afraid of Cyber-Crime than younger people? One explanation offered by Warr (1984) is that older people place greater value on property. That is, older people are more afraid than younger people of losing property. Computer systems, and debit or credit card represent property that older people are afraid of losing.

However, the above explanation of the relationship of age and fear of Cyber-Crime can hold true only for males. For females, it is the younger not the older who are more afraid of Cyber-Crime. Model 3 in table 5.3 shows that younger females are more fearful of Cyber-Crime than older. Ferraro (1995) challenges other studies that claim that older people are more fearful of crime than younger. Ferraro (1995) suggests that older people are not more fearful than younger people. Younger people are more afraid of different types of crimes such as burglary and sexual assault (Ferraro, 1995). It could be that younger females are afraid of sexual assault, and they somehow associate it with Cyber-Crime.

As table 5.3 indicates, race, having children with access to the Internet, and knowing victim variables were not significant. So, I ran another model, a parsimonious model, as table 6.4 shows, which includes only the variables that have significant effects on fear of Cyber-Crime.

As table 6.4 shows, the mean score of fear of Cyber-Crime is 0.264 units higher for females than males, controlling for all other variables in the model. The mean score of fear of Cyber-Crime is 0.245 units higher for those who have been victimized by Cyber-Crime than those who have not been victimized controlling for all other variables. The mean score of fear of Cyber-Crime is 0.160 units higher for those who feel that Cyber-Crime is a serious crime compared to those who don't, when holding all other variables constant. Age had no statistically significant effects on fear of Cyber-Crime<sup>2</sup>.

Based on the F-statistic (7.457), which is significant at the .001 level, the overall model is good. The variables in the model explain 3.7% of the variance in fear of Cyber-Crime.

---

<sup>2</sup> I ran different models and I found that age seems to work better with have children with access to the Internet. That is, when I included this variable in the model, age turned significant.



Table 6.4 OLS Regression of Fear of Cyber-Crime

Variables	Model 1	
	<i>b</i>	<i>t</i>
Age <sup>1</sup>		
<25 years-old	-0.220	0.110
25-50 years-old	-0.022	0.734
Gender <sup>2</sup>	0.264***	4.111
Cyber-Crime Victimization <sup>3</sup>	0.245***	3.676
Perceived eriousness <sup>4</sup>	0.160*	2.277
R <sup>2</sup>	0.037	
F-Statistic	7.457	
df	5	
n	985	

\*P<.05; \*\*\*P<.001

Reference categories: 1) >50 years-old; 2) Male; 3) Not victimized; 4) No seriousness.

### Conclusion

This study made use of a national survey that is considered to be the first survey about Cyber-Crime victimization among U.S. adults living in households with Internet access. The study aimed to uncover the factors that impact computer virus victimization, Cyber-Crime victimization, and fear of Cyber-Crime.

Two domains in the criminology literature were utilized to investigate Cyber-Crime victimization: routine activity theory and fear of crime. These two domains were

applied to Cyber-Crime victimization and fear as tools to assess the factors that impact Cyber-Crime victimization and fear. Different conclusions can be drawn from this study:

1. Risk exposure, which is reflected in the frequency of using the Internet and duration, was a determinant of victimization of computer virus and Cyber-Crime.
2. People who have children with access to the Internet are more likely to report computer virus victimization, but not Cyber-Crime victimization.
3. Suitable targets represented by personal information (id-target), and credit/debit cards numbers (money-target) also determine Cyber-Crime victimization.
4. In cyberspace, the convergence of time and space, which are necessary for a crime to occur, takes place, but in a different way than in the real world. In cyberspace, the place is the Internet, and time eventually provides a virus or a spy-ware, and the crime does not require an offender to be present.
5. Gender has an effect on both computer virus victimization and Cyber-Crime victimization. That is, males are more victimized than females.
6. Routine activity theory variables have explanatory power in predicting computer virus and Cyber-Crime victimization. When routine activity variables were included (money-target and id-target), the effects of age, education, and children with access to the Internet on Cyber-Crime victimization are wiped out.
7. Although females were less likely to be victimized, they were more afraid of Cyber-Crime than males. Because females have generality of fear, it could be that they somehow associate Cyber-Crime with sexual crime. Getting a virus or being

hacked increases the fear that their personal information and identity might be stolen, and, hence, they might be stalked or harassed.

8. The effect of victimization of Cyber-Crime on fear of Cyber-Crime differs by gender. Females who are victimized by Cyber-Crime have higher levels of fear of Cyber-Crime than males. Females have generality of fear and it could be that they somehow associate Cyber-Crime with sexual crime even though they are less likely to be victimized. But, when they are victimized they might reinforce the generality of fear.
9. Previous victimization increases fear of Cyber-Crime. Being victimized by Cyber-Crime may cause negative consequences for victims and results in a “sensitizing effect”, which has an impact on fear of Cyber-Crime.
10. When people think that Cyber-Crime is a serious crime, they become more fearful of Cyber-Crime than those who do not. If Cyber-Crime is perceived as a serious crime, then people will associate it with traditional crime, which they fear.
11. Indirect victimization (knowing someone who was victimized) did not predict fear of Cyber-Crime. Knowing someone who was victimized did not reinforce one’s sense of vulnerability to victimization. People may think that they are better than others in terms of protection they have in their computers, or they may think such a crime is very rare and is unlikely to happen to themselves.
12. Having children with access to the Internet did not predict fear of Cyber-Crime. One explanation is that the dependent variable, fear of Cyber-Crime, does not

include any item or question asking about the safety of one's children (Warr and Ellison, 2000).

13. Older people have a higher level of fear of Cyber-Crime than younger people.

One explanation offered by Warr (1984) is that older people place greater value on property. That is, older people are more afraid than younger people of losing property. Computer systems, and debit or credit card are valuable property older people are afraid of losing. But, for females, it is the younger not the older who are more afraid of Cyber-Crime. It could be that younger females are afraid of sexual assault and they somehow associate it with Cyber-Crime.

#### Theoretical and Policy Implications

This study is the first to investigate Cyber-Crime victimization and fear among US household adults Internet users. Two domains in criminology were applied to study Cyber-Crime victimization: routine activity theory and fear of crime. Several implications can be drawn from the current study.

The findings from analysis on computer virus victimization and Cyber-Crime victimization demonstrate that routine activity theory has explanatory power in predicting victimization. Risk exposure and suitable targets have significant influences on victimization that persist in all logistic regression models. This finding implies that there is continuity between the real world and the virtual world crimes (Yar, 2005). That is, routine activity theory was developed to study traditional crime, but the current study shows that the theory has the potential to be adapted to cyberspace. This means that

routine activity theory can be applied to a wide range of deviant behavior. Although Cyber-Crime is a unique crime, what motivates offenders in the real world also motivates them in cyberspace.

As for policy implication, since the current study is the first study to investigate Cyber-Crime victimization, more research is necessary before any policy implications can be recommended. This study found that the more people use the Internet and the longer they stay online (exposure), the more likely they will be victimized. It is not logical to advise people to use Internet less frequently or not to use it at all in order to protect themselves from being victimized. We live in a new informational age. The advantages that the Internet has, such as the ease to communicate with people, and shop, makes the Internet indispensable to people. Now many companies rely heavily on the Internet for their business. Also, the number of users of the Internet is increasing, and the new generation of people will become even more computer literate.

Given the importance of the Internet, and the fact that law enforcement has fallen behind offenders in the informational age, policy makers should develop different tools that enable them to serve as capable guardians that inhibit any crimes over the Internet.

The study found that the more people divulge their id and money information, the more likely they become victimized. This finding has an implication. Doing different activities on the Internet (buying, selling, shipping) sometimes entails Internet users to use and divulge their identity in order to complete a transaction. One recommendation to

protect Internet users from being victimized is to encrypt<sup>3</sup> the confidential information (www.geocities.com/Sarah82/cybercrime.html). Another recommendation is that when an Internet user wants to buy something online, instead of using his or her credit/debit card, he or she could ask his credit card carrier to issue a temporary credit card only valid for one certain transaction. This recommendation does not prevent Internet fraud from occurring, but it reduces its probability.

The fear of crime literature has proven to be a valid tool in predicting fear of Cyber-Crime. The study found that gender, previous victimization and perceived seriousness have significant effects on fear of Cyber-Crime. These variables that predicted fear of traditional crime also predict fear of Cyber-Crime. This implies that there is continuity between the real world and the virtual world, i.e., cyberspace, crimes. There is little difference between traditional crime and Cyber-Crime in terms of how people perceive or feel about crime. Also, many respondents feel that Cyber-Crime is a serious crime that entails attention from policy makers.

Fear of Cyber-Crime should be minimized or it may impact Internet usage. When people develop anxiety or dread about the Internet, they may stop or reduce using it. Both of these consequences will have a negative impact on the Internet, and, thus, business. When people stop shopping online due to fear, business that is established on the Internet may run out of business. So, is it possible to reduce fear of Cyber-Crime?

The study found that one of the factors that increase fear of Cyber-Crime is victimization. So, if we can reduce victimization, then, we can reduce fear. As discussed

---

<sup>3</sup> Encryption means "the process of converting a message from its original form into indecipherable or scrambled form" ( Britz, 2004. P 160).

above, policy makers should develop different tools that enable them to work as capable guardians that inhibit any crime over the Internet. Also, another tool that should be adopted by Internet users is encryption which protects important and private information of Internet users.

The study found that when people think or feel that Cyber-Crime is a serious crime, they become more fearful of Cyber-Crime. This finding has an implication for criminology and policy makers. Although Cyber-Crime is a new type of crime, it is increasing faster than traditional or street crime. So, more research should be done to unravel this phenomenon. What makes Cyber-Crime important and worth investigation by criminologists is that victims of Cyber-Crimes are increasing more quickly than we can detect, arrest, and prosecute cyber-criminals. Being a serious crime, policy makers should create rules and tools to detect, arrest, and prosecute cyber-criminals by advancing law enforcement and training law enforcement personnel to cope with the technology that is utilized by cyber-criminals.

### Future Research

As discussed in the methodology section, there are several limitations to the current study. One of these limitations is that the absence of a capable guardian couldn't be tested in this study. This limitation prevented the study from fully testing routine activity theory. Future research should include the variable (the absence of a capable guardian) by asking all respondents if they use any anti-virus, anti-spam, or anti-spy software to protect their computer system. This will help test routine activity theory more fully and help determine how victimization of Cyber-Crime happens. Also, this allows having a real measure of capable guardian instead of just assuming the measure is given or not.

With regard to Cyber-Crime, the measure of perceived risk couldn't be tested, because the survey did not include it. In the fear of crime literature, perceived risk is one of the predictors of fear of crime. Future research should include the measure of perceived risk of Cyber-Crime by asking all respondents “ how likely you think Cyber-Crime might happen to you?”

Perceived seriousness is another predictor of fear of crime, as the literature suggests. Although a valid measure of perceived seriousness is used in the current study, future research is recommended to specify the seriousness of each type of Cyber-Crime as felt by survey respondents. Operationalizing perceived risk and perceived seriousness of Cyber-Crime as recommended, future research can test each type of Cyber-Crime in terms of how serious it is and how likely is it to happen. This will enhance the research on the fear of Cyber-Crime.



The growing interest in fear of crime is attributed to concern about the consequences of the fear of crime, including personal anxiety (Hale, 1996). Although the consequences of fear of Cyber-Crime are outside the scope of the current study, I recommend future research to study how fear of Cyber-Crime affects the usage of the Internet, and in turn, affects Cyber-Crime victimization.

I developed tentative models to show how fear of Cyber-Crime affects using the Internet, and Cyber-Crime victimization. In the first model (see figure 6-a), I predict fear of Cyber-Crime by Cyber-Crime victimization, knowing victims, having children who have access to the Internet, gender (females), perceived seriousness, an interaction effect of age \*gender, and an interaction effect of gender\*Cyber-Crime victimization. These independent variables are expected to have positive relationships with fear of Cyber-Crime controlling for age, race, income and education variables. This model has already been tested by the current study.

In the second model (see Figure 6-b), I assess the effect of fear of Cyber-Crime on frequency, duration, id-target, and money-target. I expect that fear of Cyber-Crime will have negative relationships with these variables. When people are fearful of Cyber-Crime, they might constrain their behavior concerning the use of the Internet. They might use the Internet less frequently, or stay online for very short time. In the third model (see Figure 4-c), I expect a feedback effect from fear of Cyber-Crime on Cyber-Crime victimization. This effect is expected to be negative. That is, fear of Cyber-Crime might decrease Cyber-Crime victimization through affecting the use of the Internet (frequency, duration, id-target, and money-target).

Cross-sectional study will not allow for testing this proposed model. So, longitudinal data is recommended. The appropriate statistical procedure to test this model (see Figure 6-c) is structural equation modeling, because it allows testing for feedback effect (non-recursive model).

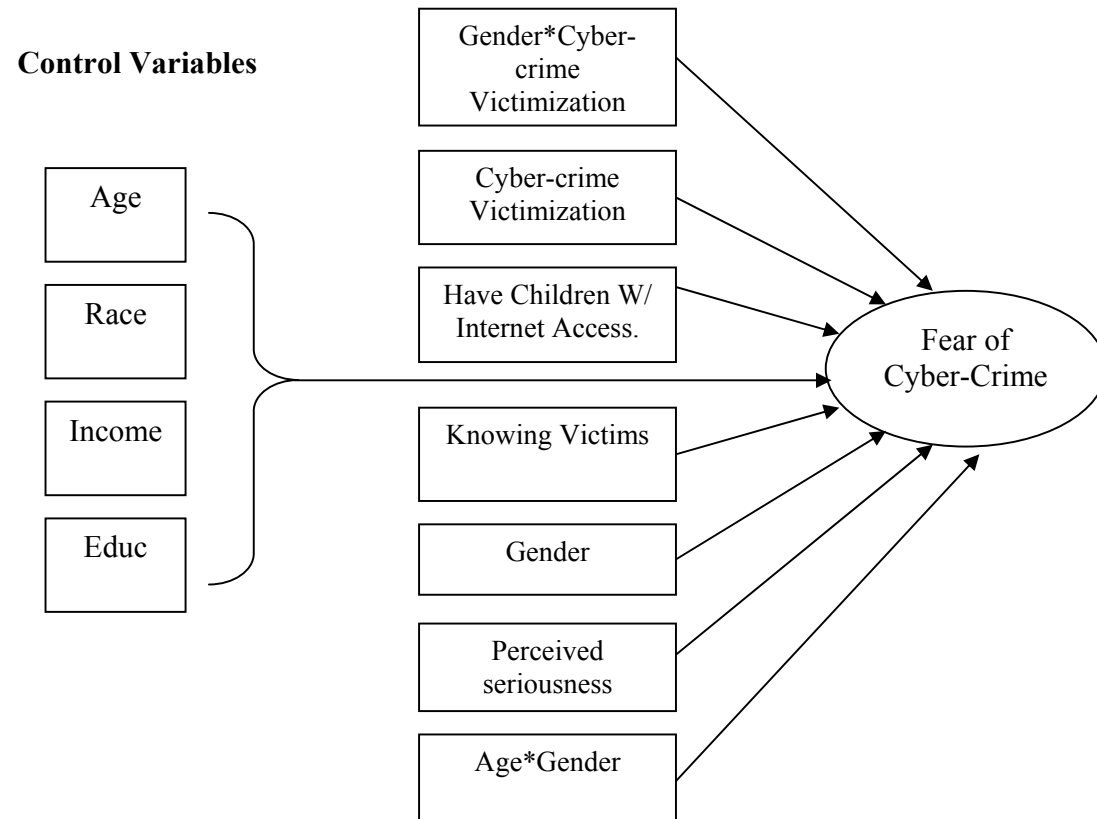


Figure 6-a. The Consequences of Fear of Cyber-Crime

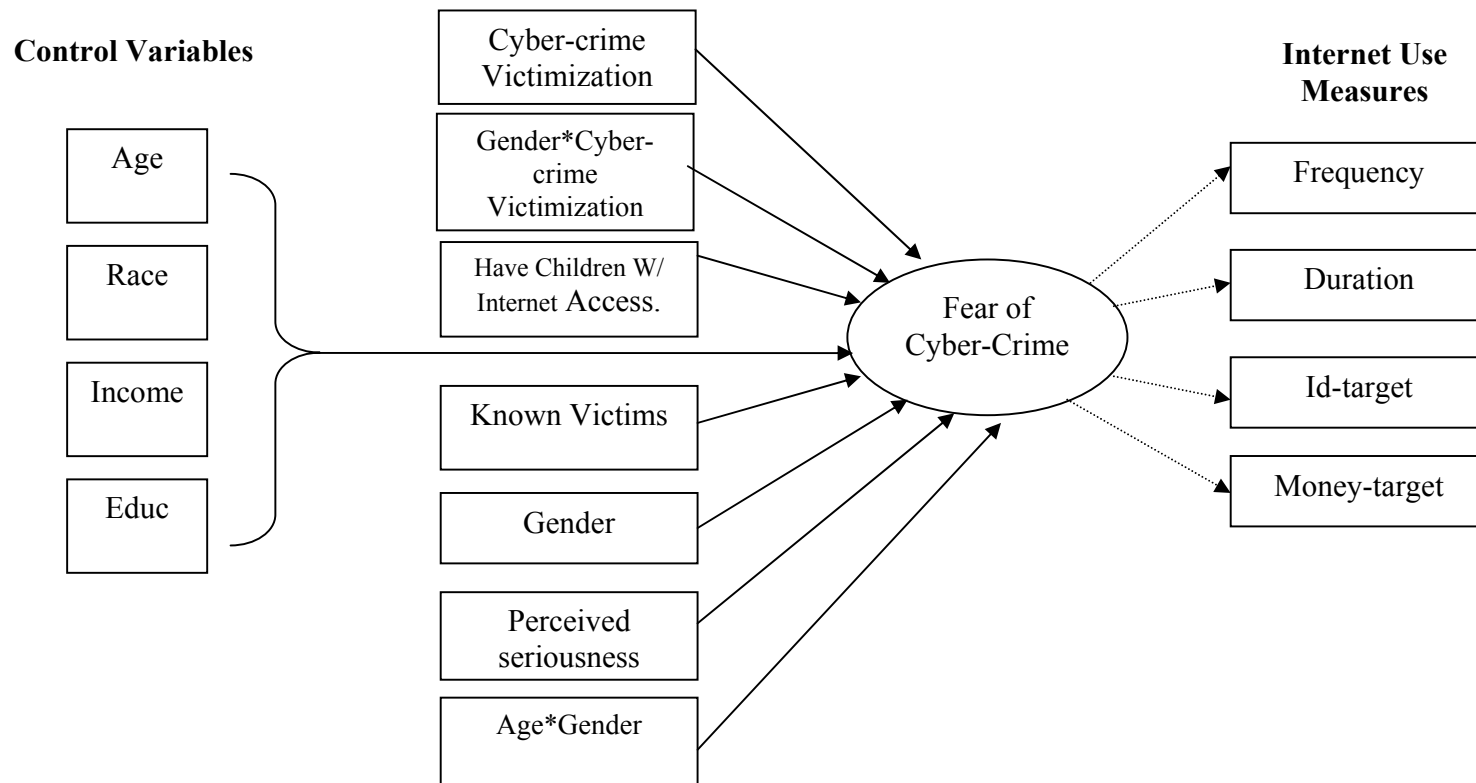


Figure 6-b. The Consequences of Fear of Cyber-Crime

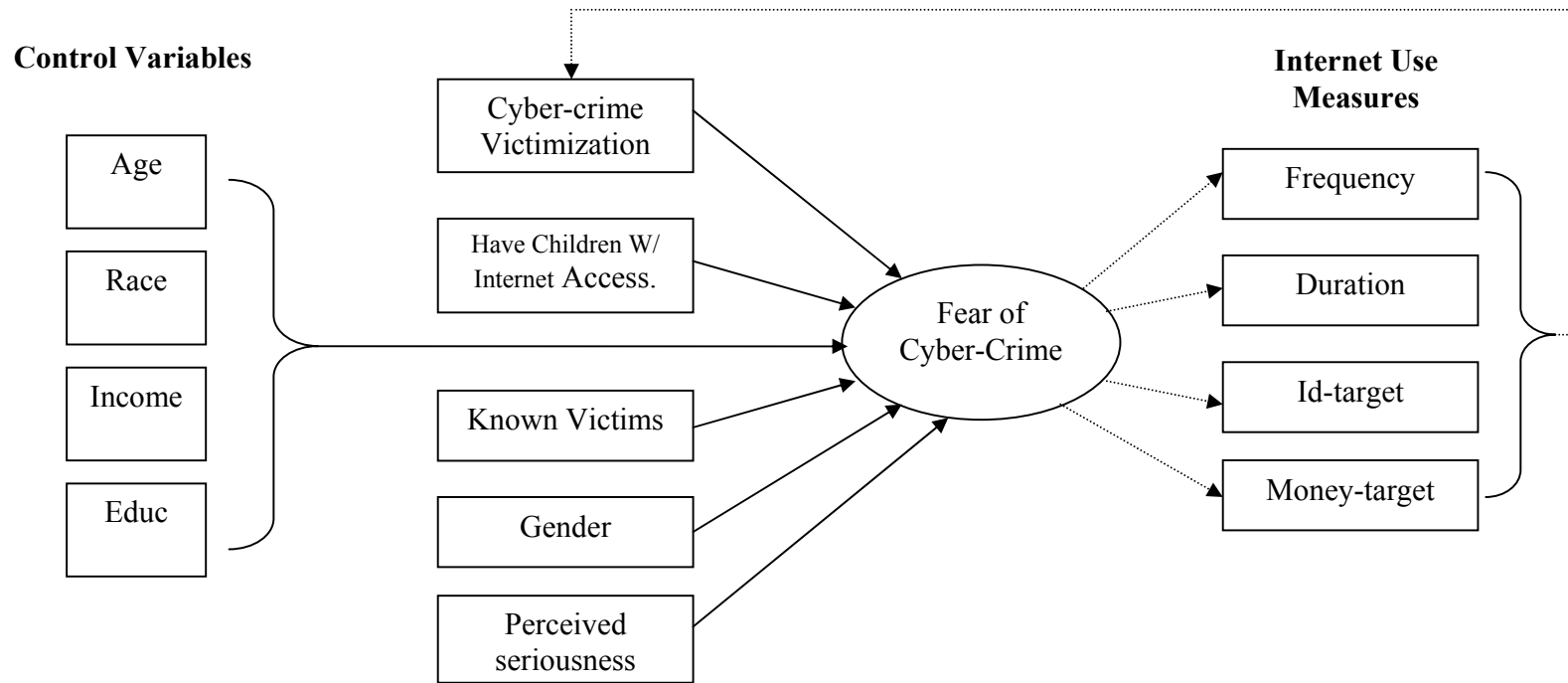


Figure 6-c. The Consequences of Fear of Cyber-Crime

## BIBLIOGRAPHY

- Barnett, Cynthia. "The Measurement of White-Collar Crime Using Uniform Crime Reporting (UCR). U.S. Department of Justice Federal Bureau of Investigation *Criminal Justice Information Services (CJIS) Division*.
- Bennett, Richard R. 1991. "Routine Activities: A Cross-National Assessment of a Criminological Perspective". *Social Forces*, 70: 147-163.
- Box, S.; Hale, C.; and Andrews, G. 1988. "Explaining Fear of Crime". *British Journal of Criminology*, 28: 340-365.
- Bureau of Justice Statistics. 2002, "Criminal Victimization 2001: Changes 2000-01 with Trends 1993-2001".
- Bureau of Justice Statistics: National Crime Victimization Survey, 2004.
- Britz, Marjie. 2004. *Computer Forensics and Cyber Crime: An Introduction*. New Jersey: Pearson Prentice Hall.
- Clinard, Marshal, and Quinney, Richard. 1973. *Criminal behavior Systems: A Typology*. New York: Free.
- Clemente, Frank; and Kleiman, Michael. 1977. "Fear of Crime in the United States: A Multivariate Analysis". *Social Forces*, 56: 519-531.
- Cohen, Lawrence E; James R. K. Kluegel; and Kenneth C. Land. 1981. "Social Inequality and Predatory Criminal Victimization: An Exposition and Test of A Formal Theory". *American Sociological Review*, 46: 505-524.
- Cohen, Lawrence E., and Marcus Felson. 1979. "Social Change and Crime Trends: A Routine Activity Approach". *American Sociological Review*, 44: 588-608.
- Colman, James Willaim. 1994. *The Criminal elite: The Sociology of White-collar Crime*. New York: St. Martin's Press.

- Edelhertz, H. 1970. "The Nature, Impact and Prosecution of White Collar Crime". Washington, D.C. National Institute of Law Enforcement and Criminal Justice. P77.
- Edelhertz, H., E. Stotland, M. Walsh, and M. Weinberg 1977. *The Investigation of White-Collar crime: A Manual for Law Enforcement Agencies*. Office of Regional Operations, Law Enforcement Assistance Administration, U.S. department of Justice, Washington, D.C. :US government Printing Office.
- Felson, Marcus; and Ronald V. Clarke. 1998. "Opportunity Makes the Thief: Practical Theory for Crime Prevention". Police Research Series. Paper 98. Research, development and Statistics Directorate. London.
- Ferraro, Kenneth F.; and LaGrange, Randy. 1987. "The Measurement of Fear of Crime". *Sociological Inquiry*, 57: 70-101.
- Ferraro, Kenneth F. 1995. *Fear of Crime: Interpreting Victimization Risk*. New York: State University Press.
- Fisher, S. Bonnie; John J. Sloan; Francis T. Cullen; and Chunmeng Lu. 1998. "Crime in the Ivory Tower: The Level and Sources of Student Victimization". *Criminology*, 36: 671-710.
- Foster, David Robert. (2004). Can The General Theory of Crime Account for Computer Offenders: Testing Low Self-Control As A Predictor of Computer Crime Offending. Unpublished Thesis. University of Maryland, College Park.
- Hale, C. 1996. "Fear of Crime: A Review of The Literature". *International Review of Victimology*, 4: 79-150.
- <http://www.InternetWorldStats.com/>
- IC3 2004 Internet Fraud - Crime Report. National White Collar Crime Center and the Federal Bureau of Investigation
- Keane, Carl. 1995. "Victimization and Fear: Assessing the Role of Offender and Offence". *Canadian Journal of Criminology*, 431-455
- LaGrange, Randy L.; Ferraro, Kenneth F.; and Supancic, Michael. 1992. "Perceived Risk and Fear of Crime: Role of Social and Physical Incivilities". *Journal of research in Crime and Delinquency*, 29: 311-334.

- Liska, Allen E., and Barbara D. Warner. 1991. "Functions of Crime: A Paradoxical Process". *The American Journal Of Sociology*, 96: 1441-1463.
- Liska, Allen E.; Lawrence, Josef J.; and Sanchirico, Andrew. 1982. "Fear of Crime as a Social Fact". *Social Forces*, 60: 760-770.
- Liska, Allen E.; Sanchirico, Andrew; and Reed, Mark D. 1988. "Fear of Crime and Constrained Behavior Specifying and estimating a Reciprocal Effects Model". *Social Forces*, 66: 827-837.
- Menard, Scott. 2002. *Applied Logistic Regression Analysis: Quantitive Applications in Social Sciences*. Thousand Oaks: Sage Publications
- Messner, Steven; and Blau, Judith. 1987. "Routine Activities and Rates of Crime: A Macro-Level Analysis". *Social forces*, 65: 1035-1052.
- Miethe, Terance; and Lee, Gary R. 1984. " Fear of Crime Among Older People: A Reassessment of the Predictive Power of Crime-Related Factors". *Sociological Quarterly*, 25: 397-415.
- Miethe, Terance; Stafford, Mark C.; and Long, J. Scott. 1987. " Social Differentiation in Criminal Victimization: A Test of Routine Activities/ Life style Theories". *American Sociological Review*, 52: 184-194.
- Mustaine, Elizabeth Ehrhardt; and Richard Tewksbury. 2000. "Comparing The Ligestyle of Vctims, Offenders, and Victim-Offenders: A Routine Activity Theory Assessment of Similareties and Differences for Criminal Incident Participants". *Sociological Focus*, 33:339-362.
- \_\_\_\_\_. 1998. "Predicting Risk of Larceny Theft Victimization: A Routine Activity Analysis Using Lifestyle Measures". *Criminology*, 36: 829-857.
- \_\_\_\_\_. 2002. "Sexual Assulat of Collage Women: A Feminist Interpretation of A Routine Activities Analysis". *Criminal Justice Review*, 27: 89-123.
- \_\_\_\_\_. 1999. "A Routine Activity Theory Explanation for Women's Stalking Victimizations". *Violence Against Women*, 5: 43-62
- Nachmias, Frankfort Chava, and David Nachmias. 1992. *Research Methods in The Social Sciences*. New York: St. Martin's.
- National and State Trends in Fraud and Identity Theft January-December 2004. Federal Trade Commission FTC



- National White Collar Crime Center. 2002 a. "Computer Crime: Computer as the Instrumentality of the Crime". Research Section.
- \_\_\_\_\_ 2002 b. "Internet Fraud". Research Section.
- \_\_\_\_\_ 2003. "Cyberstalking". Research Section.
- Ogilvie, Emma. 2000. "Cyberstalking". *Australian Institute of Criminology: Trends & Issues in Crime and and Criminal Justice*.
- Ortega, Suzanne T.; and Myles, Jessie L. 1987. "Race and Gender Effects on Fear of Crime: An Interactive Model With Age". *Criminology*, 25: 133-152.
- Rader, Nicole E. 2004. "The Threat of Victimization: A Theoretical Reconceptualization of Fear of Crime". *Sociological spectrum*, 24: 689-704.
- Roche, Edward M., Nostrand, George Van, and Kay, Jeffery H. 2003. Information Systems, Computer Crime, and Criminal justice. New York: Barraclough Ltd.
- Rodgers, Karen; and Georgia Roberts. 1995. "Women's Non-Spousal Multiple Victimization: A Test of The Routine Activities Theory". *Canadian Journal of Criminology*, 363-391.
- Rogers, Marcus Kent. (2001). A social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Explratory Study. Unpublished Dissertation. The University of Manitoba (Canada).
- Rountree, Palema Wilcox; and Land, Kenneth C. 1996. "Perceived Risk Versus Fear of Crime: Empirical Evidence of Conceptually Distinct Reactions in Survey data". *Socila Forces*, 74: 1353-1376.
- Schell, Bernadette H.; and John L. Dodge. 2002. The Hacking of America. Westport, Connecticut: Quorum.
- Shapiro, Suzan P. 2001."Collaring the Crime, Not the Criminal: reconsidering the Concept of White-Collar Crime". Pp21-31 in *Crimes of Privilege: Reading in White-Collar Crime*, edited by Neal Shover and John Paul Wright.
- Scharger, L. S., and Short, J. F. 1987. "Toward A Sociological of Organizational crime. *Social Problems*, 25: 407-419.

- Skinner, W. F., and Fream, A. M. 1997. "A Social Learning Theory Analysis of Computer Crime Among College Students". *Journal of Research in Crime and Delinquency*, 34: 495-518.
- Smith, Lynn Newhart; and Gary D. Hill. 1991. "Perceptions of Crime Seriousness and fear of Crime." *Sociological Focus*, 24: 315-327.
- Stahura, John M.; Sloan, J. III. 1988. "Urban Stratification of Places, routine Activities and Suburban Crime Rates". *Social forces*, 66: 1102-1118.
- Sutherland, Edwin H. 1940. "White-collar Criminality". *American Sociological Review*, 5: 1-12.
- 2003 the National Fraud Information Center
- Torosyan, Angela (2003). Cyber Crime Programs By Satae and Local Law Enforcement: A preliminary Analysis of A Narional Survey. Unpublished Thesis. California State University.
- Tyler, T.R. 1980. "Impact of directly and Indirectly Experienced Events: The Origin of Crime Related Judgments and behaviors". *Journal of Personality and Social Psychology*, 39:13-28.
- United Nations Crime and Justice Information Network UNCJIN, 1999
- U.S. Department of Justice, Federal Bureau of Investigation. 1989. White Collar Crime: A Report to the Public. Washington, D.C.: government Printing Office.
- Wall, David S. 2005 "The Internet as a Conduit for Criminal Activity." Pp. 77-98 in *Information Technology and the Criminal Justice System*, edited by April Pattavina. Sage publications.
- Warr, Mark. 1991. "America's Perceptions of Crime and Punishment". Pp5-19 in *Criminology: A Contemporary Handbook*, edited by Josef F. Sheley. California: Wadsworth Publishing Company.
- \_\_\_\_\_ 1984. "Fear of Victimization: Why Are Women and the Elderly More Afraid?". *Social Science Quarterly*, 65: 681-702.
- Warr, Mark; and Stafford, Mark. 1983. "Fear of Victimization: A Look at the Proximate Causes". *Social forces*, 61: 1033-1043.

Warr, Mark; and Ellison, Christopher G. 2000. "Rethinking Social reactions to Crime: Personal and Altruistic Fear in Family Housholds". *American Journal of Sociology*, 106: 551-578.

Yar, Majid. 2005. "The Novelty of Cybercrime". *European Society of Criminology*, 2: 403-427.

Consumer Reports. 2005. V: 70

Ward, Mark Technology Correspondent, BBC News website, 2004

<http://rf-web.tamu.edu/security/secguide/V1comput/Intro.htm>

<http://www.Surveysampling.com>

<http://www.internetfraud.usdoj.gov/#What%20Is%20Internet%20Fraud>

<http://www.davislogic.com/cybercrime.htm#Cybercrime>

<http://www.ncvc.org/ncvc/main.aspx?dbName=DocumentViewer&DocumentID=32458>

<http://www.davislogic.com/cybercrime.htm#Cybercrime>; NW3C, 2003

<http://www.haltabuse.org/index.shtml>

<http://www3.ca.com/Solutions/Collateral.asp?CID=41607&ID=156>

[www.geocities.com/Sarah82/cybercrime.html](http://www.geocities.com/Sarah82/cybercrime.html)

## APPENDIX A

## Questionnaire

## 2004 National Cyber Crime Survey

Question Intro

Do you use a computer with Internet access at home or at work?

1. Yes
2. No
3. Don't Know/Not Sure
4. Refused

Question homnetac

Do you have access to the Internet on your home computer?

1. Yes
2. No
3. Don't Know/Not Sure
4. Refused

Question noftnhom

On average, how often would you say you get on the Internet at home?

1. A few times per year
2. Once or twice a month
3. Once or twice a week
4. Several days a week
5. Once a day
6. Several times each day
7. NEVER
8. Don't Know/Not Sure
9. Refused

## Question howlong

When you use the Internet at home, how long do you usually stay online at one time?

1. 30 minutes or less
2. 1 hour
3. 1-2 hours
4. 2-3 hours
5. 3 or more hours
6. Don't Know/Not Sure
7. Refused

## Question emailhom

Do you have access to an e-mail account on your home computer?

1. Yes
2. No
3. Don't Know/Not Sure
4. Refused



Question pcatwrk

Do you use a computer at work?

1. Yes
2. No
3. Don't Know/Not Sure
4. Refused

Question netacwrk

Do you have access to the Internet on your work computer?

1. Yes
2. No
3. Don't Know/Not Sure
4. Refused

## Question ofnetwrk

On average, how often do you get on the Internet at work?

1. A few times per year
2. Once or twice a month
3. Once or twice a week
4. Several days a week
5. Once a day
6. Several times each day
7. NEVER
8. Don't Know/Not Sure
9. Refused

## Question lonetwrk

When you use the Internet at work, how long do you usually stay online at one time?

1. 30 minutes or less
2. 1 hour
3. 1-2 hours
4. 2-3 hours
5. 3 or more hours
6. Don't Know/Not Sure
7. Refused

Question emailwrk

Do you have access to an e-mail account on your work computer?

1. Yes
2. No
3. Don't Know/Not Sure
4. Refused

Question comwfrns

How much of your communications with friends, family, and colleagues is done via e-mail?

1. almost all of it
2. most of it
3. about half of it
4. about a third of it
5. a small amount
6. none at all
7. Don't Know/Not Sure
8. Refused

Question usedebit

Have you ever used a debit or credit card to buy something over the Internet?

1. Yes
2. No
3. Don't Know/Not Sure
4. Refused

Question paybill

Do you currently pay any bills over the Internet?

1. Yes
2. No
3. Don't Know/Not Sure
4. Refused

NOTE: For example: electric bill, phone bill, utility bill, etc.

Question gotvirus

Have you ever received a computer virus over the Internet?

1. Yes
2. No
3. Don't Know/Not Sure
4. Refused

Question victm

Have you ever been the victim of a computer-related fraud or crime?

1. Yes
2. No
3. Don't Know/Not Sure
4. Refused

## Question typecrim

Which of the following happened to them?

Internet fraud or scam offering bogus goods or services for money,  
Identity theft like theft of your debit/credit card or social security number,  
Securities fraud or stock manipulation,  
Cyberstalking or cyberharassment (via email for example),  
Extortion or blackmail via Internet, or  
Computer hacking (computer damage by amateur hackers)  
Other (Specify):  
THAT IS ALL - GO TO NEXT QUESTION  
DON'T KNOW/NOT SURE  
REFUSED

## Question antiv

Do you use any anti-virus, anti-spam, or anti-spy software to protect your computer system?

1. Yes
2. No
3. Don't Know/Not Sure
4. Refused

## Question resvic

Which of the following has happened to you?

Internet fraud or scam offering bogus goods or services for money,  
Identity theft like theft of your debit/credit card or social security number,  
Securities fraud or stock manipulation,  
Cyberstalking or cyberharassment (via email for example),  
Extortion or blackmail via Internet, or  
Computer hacking (computer damage by amateur hackers)  
Other (Specify):  
THAT IS ALL - GO TO NEXT QUESTION  
DON'T KNOW/NOT SURE  
REFUSED

## Question famvict

Has one of your family members or friends ever been the victim of a computer-related crime?

1. Yes
2. No
3. Don't Know/Not Sure
4. Refused

Question doneet

Which of the following have you done using the Internet?

Researched travel and/or lodging information  
 Bought airline tickets or hotel rooms  
 Rented a car  
 Bought books, movies, or music  
 Bought food items  
 Bought or had flowers sent  
 Paid bills (electricity, phone, gas, etc.)  
 Checked or made financial investments  
 Researched cars you might buy  
 Advertised a car you want to sell  
 Bought a car  
 Taken a web-based class for high school or university credit  
 Scheduled classes at a high school or university  
 Used an on-line auction site  
 Researched a specific health-related issue  
 Set up a web page  
 Looked for jobs/employment  
 Looked to hire someone  
 Participated in a "chat room"  
 THAT IS ALL - GO TO NEXT QUESTION  
 NONE OF THESE  
 DON'T KNOW/NOT SURE  
 REFUSED

Question INTRsecu

For each of the following computer security items, please tell me whether you are not at all concerned, somewhat concerned, or very concerned.



Question consvir

That you might receive a virus that would damage your computer system.  
Would you say you are:

1. Not at all concerned,
2. Somewhat concerned, or
3. Very concerned
4. Don't Know/Not Sure
5. Refused

Question conshack

That your computer might be accessed/hacked by other users.

1. Not at all concerned
2. Somewhat concerned
3. Very concerned
4. Don't Know/Not Sure
5. Refused

NOTE: Repeat answers 1 through 3 if necessary.

## Question concard

About entering your debit or credit card numbers over the Internet.

1. Not at all concerned
2. Somewhat concerned
3. Very concerned
4. Don't Know/Not Sure
5. Refused

NOTE: Repeat answers 1 through 3 if necessary.

## Question conporn

About issues related to Internet pornography.

1. Not at all concerned
2. Somewhat concerned
3. Very concerned
4. Don't Know/Not Sure
5. Refused

NOTE: Repeat answers 1 through 3 if necessary.

## Question conchild

That children might access pornographic websites on the Internet.

1. Not at all concerned
2. Somewhat concerned
3. Very concerned
4. Don't Know/Not Sure
5. Refused

NOTE: Repeat answers 1 through 3 if necessary.

## Question convict

That you might become a victim of a computer-related crime.

1. Not at all concerned
2. Somewhat concerned
3. Very concerned
4. Don't Know/Not Sure
5. Refused

NOTE: Repeat answers 1 through 3 if necessary.

## Question terror

That persons from the U.S. or from another country might try to damage important state and federal computer systems.

1. Not at all concerned
2. Somewhat concerned
3. Very concerned
4. Don't Know/Not Sure
5. Refused

NOTE: Repeat answers 1 through 3 if necessary.

## Question INTRatt

For each of the following items, tell me if you strongly agree, somewhat agree, somewhat disagree, or strongly disagree.

## Question loctrain

My local law enforcement agencies are trained and equipped to deal with computer-related crimes.

1. Strongly agree
2. Somewhat agree
3. Somewhat disagree
4. Strongly disagree
5. Undecided/Don't Know
6. Refused

NOTE: Repeat answers 1 through 4 if necessary.

## Question statrain

My state-level law enforcement agencies are trained and equipped to deal with computer-related crimes.

1. Strongly agree
2. Somewhat agree
3. Somewhat disagree
4. Strongly disagree
5. Undecided/Don't Know
6. Refused

NOTE: Repeat answers 1 through 4 if necessary.

Question serious

In general, our criminal justice system doesn't treat computer-related crimes as seriously as street crimes like burglary or robbery.

1. Strongly agree
2. Somewhat agree
3. Somewhat disagree
4. Strongly disagree
5. Undecided/Don't Know
6. Refused

NOTE: Repeat answers 1 through 4 if necessary.

Question viewarst

A person caught VIEWING Internet child pornography should be arrested.

1. Strongly agree
2. Somewhat agree
3. Somewhat disagree
4. Strongly disagree
5. Undecided/Don't Know
6. Refused

NOTE: Repeat answers 1 through 4 if necessary.

## Question dlodarst

A person caught DOWNLOADING and storing Internet child pornography on their computer should be arrested.

1. Strongly agree
2. Somewhat agree
3. Somewhat disagree
4. Strongly disagree
5. Undecided/Don't Know
6. Refused

NOTE: Repeat answers 1 through 4 if necessary. Downloading means they copy it to their own computer.

## Question distarst

A person caught distributing Internet child pornography should be arrested.

1. Strongly agree
2. Somewhat agree
3. Somewhat disagree
4. Strongly disagree
5. Undecided/Don't Know
6. Refused

NOTE: Repeat answers 1 through 4 if necessary.

## Question hackarst

A person caught hacking into your computer from a remote location, should be arrested.

1. Strongly agree
2. Somewhat agree
3. Somewhat disagree
4. Strongly disagree
5. Undecided/Don't Know
6. Refused

NOTE: Repeat answers 1 through 4 if necessary.

## Question hackgov

A person caught hacking into a local, state, or federal computer system, should be arrested.

1. Strongly agree
2. Somewhat agree
3. Somewhat disagree
4. Strongly disagree
5. Undecided/Don't Know
6. Refused

NOTE: Repeat answers 1 through 4 if necessary.



## Question monitor

Employers should monitor their employees' computer use, including the websites they access.

1. Strongly agree
2. Somewhat agree
3. Somewhat disagree
4. Strongly disagree
5. Undecided/Don't Know
6. Refused

NOTE: Repeat answers 1 through 4 if necessary.

## Question empfird

If an employee is caught viewing Internet pornography on their work computer, they should be fired.

1. Strongly agree
2. Somewhat agree
3. Somewhat disagree
4. Strongly disagree
5. Undecided/Don't Know
6. Refused

NOTE: Repeat answers 1 through 4 if necessary.

## Question redemail

Employers should be able to read all email messages sent and received by employees.

1. Strongly agree
2. Somewhat agree
3. Somewhat disagree
4. Strongly disagree
5. Undecided/Don't Know
6. Refused

NOTE: Repeat answers 1 through 4 if necessary.

## Question pornlib

The viewing of Internet pornography on computers at public libraries should be considered a crime.

1. Strongly agree
2. Somewhat agree
3. Somewhat disagree
4. Strongly disagree
5. Undecided/Don't Know
6. Refused

NOTE: Repeat answers 1 through 4 if necessary.

Question viewcrim

People who view Internet pornography are more likely to commit sexual crimes.

1. Strongly agree
2. Somewhat agree
3. Somewhat disagree
4. Strongly disagree
5. Undecided/Don't Know
6. Refused

NOTE: Repeat answers 1 through 4 if necessary.

Question adutview

Adults should be able to view Internet CHILD pornography in the privacy of their homes.

1. Strongly agree
2. Somewhat agree
3. Somewhat disagree
4. Strongly disagree
5. Undecided/Don't Know
6. Refused

NOTE: Repeat answers 1 through 4 if necessary.

Question adutporn

Adults should be able to view Internet adult pornography in the privacy of their homes.

1. Strongly agree
2. Somewhat agree
3. Somewhat disagree
4. Strongly disagree
5. Undecided/Don't Know
6. Refused

NOTE: Repeat answers 1 through 4 if necessary.

Question distpris

People who make, market, or distribute Internet CHILD pornography should be sent to prison.

1. Strongly agree
2. Somewhat agree
3. Somewhat disagree
4. Strongly disagree
5. Undecided/Don't Know
6. Refused

NOTE: Repeat answers 1 through 4 if necessary.

## Question nopun

Persons convicted of committing computer-related crimes are not punished as severely as they should be.

1. Strongly agree
2. Somewhat agree
3. Somewhat disagree
4. Strongly disagree
5. Undecided/Don't Know
6. Refused

NOTE: Repeat answers 1 through 4 if necessary.

## Question notdan

People who commit computer-related crimes are not as dangerous to the public as traditional street criminals like burglars and robbers.

1. Strongly agree
2. Somewhat agree
3. Somewhat disagree
4. Strongly disagree
5. Undecided/Don't Know
6. Refused

NOTE: Repeat answers 1 through 4 if necessary.

Question intrdemo

Finally, I would like to ask you a few background questions.

Press Any Key to Continue.

Question yrborn

In what year were you born? 19

NOTE: Enter last 2 digits; if BEFORE 1901 enter 0; DON'T KNOW 87; REFUSED 88.

## Question marital

What is your marital status?

1. Married
2. Single, never married
3. Living with someone but not married
4. Divorced
5. Separated
6. Widowed
7. Refused

## Question children

Do you have any children?

1. Yes
2. No
3. Don't Know/Not Sure
4. Refused

## Question income

I am going to read some income categories, stop me when I get to the one that best describes your total 2003 household income BEFORE taxes.

1. Less than \$10,000
2. 10 - \$20,000
3. 20 - \$40,000
4. 40 - \$60,000
5. 60 - \$80,000
6. 80 - \$100,000
7. More than \$100,000
8. Don't Know/Not Sure
9. Refused

## Question Thanks

This completes our interview, thank you for your cooperation.  
Good Bye.

NOTE: If you are not sure about the respondent's gender ask now.

Press Any Key To Continue.



Question sex

What is the respondent's gender?

1. Male
2. Female
3. Couldn't tell for sure

## APPENDIX B

Table B.1 Cross-Tabulation of Cyber-Crime Victimization by Selected Variables

Variables	Computer virus		Computer-related fraud or crime		Identity fraud or scam		Identity theft		Securities fraud		Cyber-stalking		Extortion or blackmail		Computer hacking	
	N	%	N	%	N	%	N	%	N	%	N	%	N	%	N	%
Age																
<25 years-old	49	54.4	6	6.7	3	50.0	1	16.7	0	0	1	16.7	0	0	2	33.3
25-50 years-old	368	65.8	49	8.8	13	26.5	25	51.0	0	0	2	4.1	4	44.0	4	8.2
> 50 years-old	322	57.7	37	6.6	14	46.7	19	51.4	1	2.7	2	5.4	0	0	2	5.4
<i>Chi-square</i>	10.506*		2.021		6.408		5.412		5.179		5.560		7.261		9.296	
Low Income	37	49.3	6	8.0	1	16.7	3	5.0	0	0	0	0	1	16.7	0	0
Mid Income	259	62.0	29	6.9	10	34.5	14	48.3	1	3.4	2	6.9	2	6.9	4	13.8
High Income	275	63.7	38	8.8	14	36.8	20	52.6	0	0	1	2.6	0	0	2	5.3
<i>Chi-square</i>	7.174		3.561		2.502		1.588		3.120		2.638		6.202		3.838	

\*Significance at p<.05

Table B.1 (Continued)

Variables	Computer virus		Computer-related fraud or crime		Identity fraud or scam		Identity theft		Securities fraud		Cyber-stalking		Extortion or blackmail		Computer hacking		
	N	%	N	%	N	%	N	%	N	%	N	%	N	%	N	%	
Frequency																	
<i>Never</i>	2	28.6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<i>A few times per year</i>	5	31.3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<i>Once or twice a month</i>	23	46.0	1	2.0	0	0	1	2.2	0	0	0	0	0	0	0	0	0
<i>Once or twice a week</i>	101	53.4	12	6.3	5	41.7	6	50.0	0	0	0	0	0	0	1	8.3	
<i>Several days a week</i>	99	59.3	6	3.6	0	0	2	33.3	0	0	2	33.3	1	16.7	2	33.3	
<i>Once a day</i>	302	65.8	41	8.9	12	29.3	25	61.0	1	2.4	2	4.9	1	2.4	1	2.4	
<i>Several times each day</i>	188	69.6	29	10.6	12	41.4	11	37.9	0	0	1	3.4	1	3.4	4	13.8	
<i>Chi-square</i>	35.431***		26.291*		6.885		6.706		2.427		10.863		4.997		8.657		

\*Significance at  $p < .05$ \*\*\*Significance at  $p < .001$

Table B.1 (Continued)

Variables	Computer virus		Computer-related fraud or crime		Identity fraud or scam		Identity theft		Securities fraud		Cyber-stalking		Extortion or blackmail		Computer hacking	
	N	%	N	%	N	%	N	%	N	%	N	%	N	%	N	%
Duration																
<i>30 Minutes or less</i>	258	55.0	22	4.7	8	36.4	9	40.9	0	0	0	0	0	0	2	9.1
<i>One hour</i>	246	66.0	28	7.5	6	21.4	18	64.3	0	0	2	7.1	0	0	1	3.6
<i>1-2 hours</i>	128	69.6	22	12.0	10	45.5	10	45.5	1	4.5	3	13.6	0	0	3	13.6
<i>2-3 hours</i>	30	71.4	5	11.9	0	0	3	60.0	0	0	0	0	1	20.0	1	20.0
<i>3 or more hours</i>	48	71.6	12	17.9	5	41.7	5	41.7	0	0	0	0	2	16.7	1	8.3
<i>Chi-square</i>	21.869**		25.180**		16.334*		12.403		12.470		14.227		22.535**		11.836	

\*Significance at  $p < .05$ \*\*Significance at  $p < .01$

## APPENDIX C

Table C.1 Logistic Regression of Computer Virus Victimization  
(Interaction Terms) (Dependent Variable: 1 =Yes)

Variables	Model 1	
	Coeffi	Wald
Age	-0.15** (0.985)	8.017
Gender <sup>1</sup> (male)	0.492** (1.636)	11243
Race <sup>2</sup> (white)	693* (1.999)	5.177
Type of Residence <sup>3</sup> (Rural)	-0.029 (0.971)	0.039
Education	0.083** (1.086)	7.250
Low Income <sup>4</sup>	-5.15 (0.597)	2.601
Mid Income	-0.053 (0.948)	0.101
Income (missing)	0.176 (1.193)	0.825
Children w/access to Internet <sup>5</sup>	0.513* (1.671)	5.078
Children w/ access to Internet (missing)	0.249 (1.283)	8.97
Frequency	0.137 (1.146)	3.816
Duration	0.203* (1.224)	5.321
Gender*Frequency	0.093 (1.097)	0.582
Gender*Duration	0.137 (1.147)	0.895
Model X <sup>2</sup>		74.809***
df		14
n		987

\*P<.05; \*\* P<.01; \*\*\*P<.001

Note: Numbers in parentheses are Exp(B)

1)female is the reference; 2) black is the reference; 3)urban is the reference;

4) high income is the reference; 5) children with no access to the Internet

Table C.2 Logistic Regression of Computer Virus Victimization  
(Interaction Terms) (Dependent Variable: 1 =Yes)

Variables	Model 1	
	Coeffi	Wald
Age	-0.014** (0.986)	7.556
Gender <sup>1</sup> (male)	0.474** (1.606)	10.614
Race <sup>2</sup> (white)	-0.512 (0.599)	0.228
Type of Residence <sup>3</sup> (Rural)	-0.049 (0.952)	0.108
Education	0.082** (1.086)	7.153
Low Income <sup>4</sup>	-0.381 (0.683)	1.349
Mid Income	-0.057 (0.945)	0.117
Income (missing)	0.180 (1.197)	0.860
Children w/access to Internet <sup>5</sup>	0.450* (1.568)	3.837
Children w/ access to Internet (missing)	0.188 (1.207)	0.503
Frequency	0.292 (1.339)	1.338
Duration	-0.443 (0.642)	2.422
Race*Frequency	-0.125 (0.882)	0.233
Race*Duration	0.758* (2.134)	6.657
Model X <sup>2</sup>		81.195***
df		14
n		987

\*P<.05; \*\* P<.01; \*\*\*P<.001

Note: Numbers in parentheses are Exp(B)

1)female is the reference; 2) black is the reference; 3)urban is the reference;  
4) high income is the reference; 5) children with no access to the Internet



Table C.3 Logistic Regression of Computer Virus Victimization  
(Interaction Terms) (Dependent Variable: 1 =Yes)

Variables	Model 1	
	Coeffi	Wald
Age	-0.014** (0.986)	7.793
Gender <sup>1</sup> (male)	0.468** (1.596)	10.406
Race <sup>2</sup> (white)	0.673* (1.961)	4.904
Type of Residence <sup>3</sup> (Rural)	0.497 (1.644)	0.820
Education	0.083** (1.087)	7.392
Low Income <sup>4</sup>	-0.542 (0.582)	2.873
Mid Income	-0.046 (0.955)	0.077
Income (missing)	0.187 (1.206)	0.930
Children w/access to Internet <sup>5</sup>	0.505* (1.657)	4.931
Children w/ access to Internet (missing)	0.237 (1.267)	0.815
Frequency	0.211** (1.235)	8.550
Duration	0.253*** (1.287)	12.789
Type of residence*Frequency	-0.120 (0.887)	1.036
Model X <sup>2</sup>		74.131***
df		13
n		987

\*P<.05; \*\* P<.01; \*\*\*P<.001

Note: Numbers in parentheses are Exp(B)

1)female is the reference; 2) black is the reference; 3)urban is the reference;

4) high income is the reference; 5) children with no access to the Internet

Table C.4 Logistic Regression of Cyber-Crime Victimization  
(Interaction Terms)(Dependent Variable: 1 =Yes)

Variables	Model 1	
	Coeffi	Wald
Age	-0.009 (0.991)	2.890
Gender <sup>1</sup> (male)	0.493** (1.636)	10.600
Race <sup>2</sup> (white)	0.700* (2.014)	5.071
Type of Residence <sup>3</sup> (Rural)	0.042 (1.043)	0.075
Education	0.054 (1.055)	2.815
Low Income <sup>4</sup>	-0.389 (0.678)	1.395
Mid Income	-0.024 (0.976)	0.019
Income (missing)	0.221 (1.247)	1.194
Children w/access to Internet <sup>5</sup>	0.428 (1.534)	3.339
Children w/ access to Internet (missing)	0.203 (1.224)	0.563
Frequency	0.099 (1.104)	1.878
Duration	0.193* (1.213)	4.454
Id-target	0.125* (1.133)	0.038
Money-Target	0.177** (1.194)	8.203
Gender*Frequency	0.1.09 (1.115)	0.770
Gender*Duration	0.041 (1.041)	0.075
Model X <sup>2</sup>		100.954***
df		16
n		987

\*P<.05; \*\* P<.01; \*\*\*P<.001

Note: Numbers in parentheses are Exp(B)

1)female is the reference; 2) black is the reference; 3)urban is the reference;  
4) high income is the reference; 5) children with no access to the Internet

Table C.5 Logistic Regression of Cyber-Crime Victimization  
(Interaction Terms) (Dependent Variable: 1 =Yes)

Variables	Model 1	
	Coeffi	Wald
Age	-0.008 (0.992)	2.547
Gender <sup>1</sup> (male)	0.483** (10.407)	1.621
Race <sup>2</sup> (white)	-0.536 (0.585)	0.259
Type of Residence <sup>3</sup> (Rural)	0.031 (1.031)	0.039
Education	0.052 (1.054)	2.685
Low Income <sup>4</sup>	-0.282 (0.754)	0.698
Mid Income	-0.032 (0.968)	0.034
Income (missing)	0.219 (1.244)	1.168
Children w/access to Internet <sup>5</sup>	0.372 (1.450)	2.492
Children w/ access to Internet (missing)	0.149 (1.161)	0.302
Frequency	0.143 (1.153)	0.331
Duration	-0.290 (0.749)	1.202
Id-target	0.130* (1.138)	4.633
Money-Target	0.179** (1.196)	8.313
Race*Frequency	-0.004 (0.996)	0.0003
Race*Duration	0.547* (1.729)	3.991
Model X <sup>2</sup>		104.834***
df		16
n		987

\*P<.05; \*\* P<.01; \*\*\*P<.001

Note: Numbers in parentheses are Exp(B)

1)female is the reference; 2) black is the reference; 3)urban is the reference;

4) high income is the reference; 5) children with no access to the Internet

Table C.6. Logistic Regression of Cyber-Crime Victimization  
(Interaction Terms) (Dependent Variable: 1 =Yes)

Variables	Model 1	
	Coeffi	Wald
Age	-0.009 (0.991)	0.100
Gender <sup>1</sup> (male)	0.478** (1.612)	10.210
Race <sup>2</sup> (white)	0.696* (2.006)	5.031
Type of Residence <sup>3</sup> (Rural)	0.262 (1.300)	0.558
Education	0.054 (1.055)	2.857
Low Income <sup>4</sup>	-0.401 (0.669)	1.479
Mid Income	-0.024 (0.976)	0.019
Income (missing)	0.223 (1.250)	1.22
Children w/access to Internet <sup>5</sup>	0.415 (1.515)	3.155
Children w/ access to Internet (missing)	0.190 (1.210)	0.500
Frequency	0.152* (1.164)	4.142
Duration	0.208** (1.232)	8.017
Id-target	0.126* (1.135)	4.444
Money-Target	0.179** (1.196)	8.417
Type of Residence*Frequency	-0.051 (951)	0.176
Model X <sup>2</sup>		100.207***
df		15
n		987

\*P<.05; \*\* P<.01; \*\*\*P<.001

Note: Numbers in parentheses are Exp(B)

1)female is the reference; 2) black is the reference; 3)urban is the reference;

4) high income is the reference; 5) children with no access to the Internet