Purdue University
Purdue e-Pubs

Open Access Theses

Theses and Dissertations

January 2015

A Predictive Model For Self-reported Computer Criminal Behavior Among College Students

Danielle M. Crimmins
Purdue University

Follow this and additional works at: https://docs.lib.purdue.edu/open_access_theses

Recommended Citation

Crimmins, Danielle M., "A Predictive Model For Self-reported Computer Criminal Behavior Among College Students" (2015). *Open Access Theses*. 1210.
https://docs.lib.purdue.edu/open_access_theses/1210

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By Danielle M. Crimmins

Entitled
A PREDICTIVE MODEL FOR SELF-REPORTED COMPUTER CRIMINAL BEHAVIOR AMONG COLLEGE STUDENTS

For the degree of   Master of Science

Is approved by the final examining committee:

Dr. Marcus Rogers
_____
Chair

Dr. John Springer

Dr. Kathryn Seigfried-Spellar

To the best of my knowledge and as understood by the student in the Thesis/Dissertation Agreement, Publication Delay, and Certification Disclaimer (Graduate School Form 32), this thesis/dissertation adheres to the provisions of Purdue University's "Policy of Integrity in Research" and the use of copyright material.

Approved by Major Professor(s): Dr. Marcus Rogers

Approved by: Dr. Marcus Rogers   7/21/2015
         Head of the Departmental Graduate Program   Date

A PREDICTIVE MODEL FOR SELF-REPORTED COMPUTER CRIMINAL

BEHAVIOR AMONG COLLEGE STUDENTS

A Thesis

Submitted to the Faculty

of

Purdue University

by

Danielle M. Crimmins

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

August 2015

Purdue University

West Lafayette, Indiana

To my wonderful family and Brian who have always supported and encouraged me.

ACKNOWLEDGEMENTS

First, I would like to thank Dr. Marcus Rogers for encouraging and motivating me through this process and also pushing me to have more confidence in myself. I am grateful for all of your help. I would like to thank Dr. Kathryn Seigfried-Spellar not only for help on my thesis but also for guidance and mentoring over the past few years. I am grateful for all of your support and guidance. Also, a big thank you to Dr. John Springer for agreeing to be a committee member and helping throughout the process. I would also like to thank Mrs. Stacy Lane for answering countless questions about deadlines and forms. I am very grateful for your help and guidance along during this process.

Last but not least, I would like to thank my support system: my family, boyfriend and friends. I feel extremely lucky to have so many amazing people supporting and encouraging me during this process. Whenever I doubted my abilities I could always count on all of you to encourage and believe in me and for that I am very grateful!

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ABBREVATIONS

ANOVA – Analysis of Variance

BIG5 – Goldberg's Modified Big 5 Personality Questionnaire

CCI – Computer Crime Index

CCI-R – Computer Crime Index – Revised

DFS – Digital Forensics

DSM – Diagnostic and Statistical Manual of Mental Disorders

EMAD – Exploitive Manipulative Amoral Dishonesty

IAT – Internet Addiction Test

IC3 – Internet Crime Complaint Center

MDKS – Moral Decision Making Scale

WWW – World Wide Web

GLOSSARY

Computer Deviant - participants in the current study who indicated on the CCI-R they

       engaged in 1 or more of the computer deviant behaviors asked on the survey

Computer Non-Deviant – participants in the current study who indicated they did not

       engage in any of the computer deviant behaviors listed on the CCI-R

Cracker – individuals who engage in hacking with malicious intent (Barber, 2001)

Digital Forensics (DFS) – "the use of scientifically derived and proven methods toward

       the preservation, collection, validation, identification, analysis and interpretation,

       documentation and presentation of digital evidence derived from digital sources

       for the purpose of facilitation or furthering the reconstruction of events found to

       be criminal, or helping to anticipate unauthorized actions shown to be disruptive

       to planned operations" (DFRWS, 2001).

Hacking – gaining unauthorized access to computer data or network

Internet Addiction- problematic, excessive or mal-adaptive use of the internet (Thombs,

       1994; Young, 1998)

Malware (malicious software) – term used to describe a wide range of destructive

       programs that can be used to harm a computer system, gain acess to

       sensitive/classified information or to commit various forms of cybercrimes (Holt

       et al. 2015; p. 80

Net-Generation (Net-Gen) – anyone born since1983 is considered part of the net

generation (Junco et al. 2007)

Virus Writing – intentionally writing or using a program that would destroy an

individual's data or infect the computer/network (ex: logic bomb)

ABSTRACT

Crimmins, Danielle M. M.S., Purdue University, August 2015. A Predictive Model for Self-reported Computer Criminal Behavior among College Students. Major Professor: Dr. Marcus Rogers.

Presently, computer crime is rampant and costly. Combating these crimes is not only focused on the technical aspect but also the individual behind the computer. Researchers agree the way to fight computer crime is to gain a better understanding of those behind the keyboard. In an effort to aid investigators in profiling computer criminals, the current study aims to add empirical literature relating to characteristics which predict computer behavior. The current study aims to test the Rogers, Seigfried and Tidke (2006) predictive model and determine if Internet addiction is related to self reported computer deviant behavior. By utilizing a snowball sampling method the current study (n=95) was comprised of 49 self reported computed deviants and 46 non-computer deviants. Over all, Internet addiction was the best predictive variable for computer behavior. Those who scored high on the Internet Addiction Test (IAT) were 1 time more likely to be self-reported computer deviants. Limitation and future research is also discussed.

CHAPTER 1. INTRODUCTION

In recent years, the world has seen dramatic advancements in new technologies;

these advancements have brought both positive and negative side effects for individuals,

business and national security. Almost 40% of the world's population is online, which is

a 20% increase from 2006 (ITU, 2013). Additionally, mobile-cellular penetration rates

stand at 96% (ITU 2013). In the annual Computer Crime report, statistics show that

269,422 computer related crimes were reported in 2014 with an overall, total loss of

$800,492,073; compared to 262,813 complaints with a loss of $784,841,611 in 2013

(IC3, 2013 & 2014). With the constant growth of computer related crime, coupled with

the vast amount of the population connected to the Internet, the need to better understand

these types of criminals is imperative. Empirical research aims to determine behavioral

characteristics that predict computer criminals. The insights offered by this research will

further add to the empirical literature on computer criminals and also aid in profiling

computer criminal for investigative purposes.

1.1   Statement of Purpose

Previous empirical research shows researchers have began to examine various

factors which may predict or be associated with computer criminal behavior. Specifically,

previous recent research has looked at different characteristics, including:

personality traits (Rogers, Seigfried, & Tidke, 2006) moral decision, self control and making and time spent online versus time spent outdoors (Hu, Zhang & Xu, 2012) as well as degree major (Seigfried-Spellar & Treadway, 2014). Additionally, researchers have examined different explanations why some computer talent results in hacking; including time spent playing games on the computer versus time spent outdoors engaging in sport activities (Hu, Chang, & Xu, 2012). Therefore, the current study aspired to add additional empirical evidence pertaining to characteristics of self-report0d computer criminal behavior among college students. Also, the current study added to the growing body of literature regarding computer criminal behavior by examining a new predicting variable: Internet addiction. This study tested the Rogers, Tidke and Seigfried predictive model, along with the addition of Internet addiction. Over use of the Internet has been linked to cyberbullying and more time spent online playing games has been linked to hacking behaviors (Hinduja & Patchin, 2008; Hu, Zhang, & Xu, 2012). The purpose of this paper is not to argue or determine whether or not Internet addiction is a true addiction but rather examine if the characteristics of internet addiction are associated with computer deviant behavior.

Two previous studies (Rogers et al. 2006a; Rogers et al. 2006b) provided mixed results. For instance, Rogers et al. (2006) found participants who were classified as computer criminals scored higher on exploitive and manipulative behavior. Contrary to this, Rogers, Seigfried (2006) found no significant different between computer criminals behavior and manipulative/exploitive scores. The two previous studies (Rogers & Seigfried, 2006; Rogers et al., 2006) also only examined self-reported computer criminal behavior among undergraduates from the same student body. This study surveyed a

variety of university students throughout the United States in effort to result in a more diverse sample. In summary, the current study sought to acquire a diverse sample, test the Rogers, Seigfried and Tidke predictive model and determine if Internet addiction characteristics are related to computer deviant behavior.

1.2   Research Question

The current study posed the following question:

1. Does the Rogers, Seigfried, Tidke model and Internet addiction predict self-reported computer criminal behavior among college students?

1.3   Assumptions

The assumptions inherit to the current study included the following:

1. Participants will fully and carefully read each question listed in the survey.

2. Participants will have a basic understanding of what each question is asking, which will be demonstrated in the instructions for each section of the survey.

3. Participants will answer all the questions honestly and free of bias.

1.4   Limitations

The focus of the current study was to examine the differences in personality characteristics, and Internet addiction of self-reported computer criminal behavior between students from across the United States. For this reason, the limitations innate to the current study were as follows:

1. The current study will include a sample of college students, both undergraduate and graduate, who are currently enrolled in universities across the United States.

2. Respondents will be asked to participate in a voluntary survey that should take approximately 15 minutes to complete.

3. Participants will not be compensated for their participation in the survey.

4. The survey will be conducted using Qualtrics online survey software.

5. The survey will be completely anonymous, and no identifying information will be linked to the participants (e.g., IP address, student ID number, etc.).

6. The survey will only examine the different personality characteristics, Internet addiction and computer behavior of the participants.

7. The survey will be comprised of the following sections: demographics, Computer Crime Inedex-Revised (CCI-R) Exploitive Manipulative Amoral Dishonesty Scale (EMAD), Goldberg's Modified Big 5 Personality Questionnaire (Big5), and the Moral Decision Making Scale (MDKS) and Internet Addiction Test (IAT).

1.5   Delimitations

The delimitations related to the current study were the follows:

1. All the participants are currently enrolled in a university or college located within the United States.

2. The current study will be conducted only for six weeks of the Spring 2015 semester or until the number of participants required is met, whichever comes first.

3. The current study will not categorize participants based on full-time or part-time status at their university or college.

4. The current study does not categorize participants based on their ethnicity or gender.

1.6   Organization

The current study includes five major chapters. Chapter 2 provides an overview of research related to computer criminal behavior and internet addiction. This begins with a historical synopsis of empirical studies on computer criminal behavior, followed by an overview of addiction and Internet addiction characteristics, and last details computer use and literacy among college students. Chapter 3 provides an in-depth overview to the methodology and framework utilized in the current study, outlining the included procedures, participants, and measurements. Chapter 4 gives a detailed description of the data analysis and subsequent results. Lastly, Chapter 5 discusses the results and provides a conclusion of the study, followed by recommendations for further research and discussion of the limitations associated with the current study.

1.7   Summary

This chapter has provided an overview to the research project by reviewing the background, significance, purpose of the study and the research question. Furthermore, the chapter outlined the assumption, limitations, and delimitations associated with the study. The chapter also provided an overview for the entire study and this document. The following chapter will outline empirical research studies related to computer criminal behavior, identify the participants, and discuss the methods of data collection.

CHAPTER 2. LITERATURE REVIEW

Research regarding computer behavior has been ongoing and gaining popularity

among researchers in recent years. This review of the literature begins with a brief history,

definitions and classifications of cybercrime followed by empirical research studies

regarding the profiling of computer criminals. As the new predicting variable measured

in the current study is Internet Addiction, a review of general addiction research followed

by Interne Addiction is presented. Finally, a review of computer use and literacy among

college students is provided.

2.1   Prevalence of Computer Crime

There has been an influx in monetary loss due to computer criminal activity in

recent years, according to the annual comprehensive report of overall cyber criminal

activity distributed by the Internet Crime Complaint Center (IC3, 2011; 2012; 2013). The

IC3 is a data-loss database which accepts online Internet crime complaints, from both

victims and third party complainant. In the IC3 2011 annual report, the report indicated

there were 207,449 computer crimes reported, totaling a loss of $485,253,871. In the IC3

2012 report, there was an 8.3% increase in monetary loss ($524,441,110) but a slight

decrease in incident reports (289,874). Similarly, in the IC3 2013 annual report there was

a continued slight decrease in complaints, with 262,813 complaints, and a similar

extreme increase in monetary loss ($781,841,611, with an increase of $257,400,501 from

2012). Presently, the 2014 reported indicated there were 269,422 complaints reported with a total loss of $800,492,073, an increase in both complaints and financial loss from 2013. More specifically, in 2014 there was an average of 22,000 complaints each month, with the average dollar loss for complaints reporting a loss of $6,472. Some complaints include Auto Fraud (total: 16,861/financial loss: $56,222,655), Government impersonation email scam (total: 8,713/financial loss: $11,334,077), and intimidation, exhortation (total: 7,923/financial loss: $16,346,239). Complaints comprised of 53% males and 47% females, with the top five states for complaints including: California, Florida, Texas, New York, Pennsylvania, and Illinois (IC3, 2014).

In another report by the Computer Security Institute, which release statistics related to cyber criminal behavior, found computer criminal behavior and monetary losses to be a current problem (Richardson, 2011). The majority of business respondents reported malware infections (67%) as the most common attack (Richardson, 2011). Other attacks reported included the following: 38.9% phishing, 24.8% password sniffing and 11.4% financial fraud (Richardson, 2011). Off all the attacks surveyed in the CSI report 57.6% resulted in a direct financial loss for the victim (Richardson, 2011).

Similarly, the 2013 Norton Report from Symanetc, data from 13,000 adults from 24 counties across the world was collected; data examined consumers online behaviors, security habits, attitudes and cost of cybercrime. Statistics found that consumers are currently more mobile than ever before, specifically 63% own smart phones and 30% own tablets (Norton Report, 2013). Nearly half (49%) of individuals use their personal devices to partake in work related activates (Norton Report, 2013). However, alarmingly, nearly half do not take necessary security precautions (i.e., utilizing security software)

(Norton Report, 2013). Additionally, the Norton Report (2013) found global cost of cybercrime to be up from $110 billion to $113 billion. Statistics (IC3, 2011; 2012; 2013;2014; Richardson, 2011; Norton Report, 2013) provided evidence that computer criminal behavior is rampant and costly.

2.2 <u>Cybercrime: Definitions, Classifications, Brief History and Types of Attacks</u>

Before understanding the profile of cyber criminals, first an understanding of the definitions and classifications surrounding cybercrime is necessary; as well as, a brief history of the Internet and hacking.

2.2.1 Definitions and Classifications

From the big-screen, Black hat (2015) to prime time television, "CSI-Cyber (2015), and headline news: " 2015 is already the year of the health care hack – and it's only going to get worse" (Washington Post, 2015), "cybercrime" is constantly being discussed, "Cybercrime" is one of the most common terms used when referring to the use of computer technology to engage in an illegal activity (Brenner, 2011; Bem et al., 2008). A computer is defined as "an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic or storage functions" (18 U.S.C 1020 (e)(1) (2006)). Cybercrime often falls into one of three categories: the computer as the target, the computer as the tool or the computer as an aspect of the commission of the crime (Brenner, 2001). The computer as the target refers to an individual breaking into or bombarding the computer, typically through hacking or cracking (Brenner, 2001). The computer as the tool to commit a crime refers to the computer as the instrument to commit a crime; an example of this include the creation or spreading of child pornography files (Brenner, 2001). The computer as an aspect of the

crime refers to the computer being a source of evidence; an example of this would be a drug dealer storing his financial transactions on his / her computer (Brenner, 2001). Additional types of cybercrime include: cyberterorrism, using technology to carry out terrorist attacks and cyberwarfare, the use of computer to achieve military or other strategic goals (Brenner, 2001). To obtain evidence admissible in court, digital forensics formed. Digital Forensics (DFS) is used to examine cases involving, but not limited to, computer intrusions, unauthorized use of corporate computers, child pornography and physical crimes where the suspect used/had a computer (Carrier, 2002).

Hacker is a common term used to describe individuals who illegally gain access to computer data or networks (Barber, 2001). Hacker however is an umbrella term to the many different types of hackers which researchers have identified. Researchers typically classify hackers based on their motive or intention, skill level or affiliation to a company, either as an insider or an outsider (Barber 2001; Holt & Shell, 2013; Rogers 2006). Although the term "hacker" was first used to describe skilled programmers, typically working at Universities and government agencies, the term eventually grew to hold negative condemnations. After computers became easily accessible and affordable, people started referring to young, curious individuals as "hackers" due to their interest in computers and how the computer worked (Holt & Shell, 2013). The curiosity of these young individuals led to pranks, which gained the attention of the authorities. The changes to the term "hacker" included both noncriminal and criminal individuals (Holt & Shell, 2013). To differentiate from those with noncriminal intent and those with criminal / malicious intent, the term "cracker" was coined. The term "cracker" refers to

individuals with malicious intent or individuals who "made a decision to do damage to people and/or companies via the Internet" (Barber, 2001).

Within the term "hacker" there is three different types, based on motive/ intention; these types include: White Hat, Black Hat and Grey Hat. White hat hackers are individuals with skilled computer abilities who use their skills and computer talent to protect/defend computers and their networks, often labeled as the "do-gooders" (Holt & Shell, 2013; Barber, 2001; Caldwell, 2011). The white hats typically use their skills to improve security for government agencies and industry through various information technology roles (Holt & Shell, 2013). White hats are also often referred to as "Ethical Hackers" because although they possess the ability to 'hack' they choose to do so ethically/legally (Caldwell, 2011). Caldwell (2011) draws attention to the need for "ethical hackers" in network security; the constant change in threat broadens the skill set of "ethical hackers", including social engineering, social networking and consumer mobile technologies. If white hats hackers portray a hero, than the black hat hacker would be classified as the villain. Black hat hackers are the malicious online hackers. Grey hat hackers refers to individuals who's motive behind hacking shifts from ethical to malicious depending upon the target; the Grey hat hacker may choose malicious actions or protective actions based on the given target (Holt & Shell, 2013).

Holt and Shell (2013) classify individuals based on their skill level, which is essential to the hacker subculture. Holt and Kilger (2008) suggest placing hackers into one of two groups; those who produce materials, such as script and tools, would be labeled as "makecrafters" and those who consume the new materials would be called "techcrafters". Individuals with an interest in hacking but who actually posses little to no

technical skills would be called "noobs" (n00bs); (Holt 2007; 2010). Additionally, those

individuals who download information with little knowledge of what the material will do

are referred to as "script kiddies" (Holt 2010, Jordan & Taylor, 1998, Taylor 1999).

Typically, "script kiddies" receive their tools from the "elite" individuals within the

hacker community; the "elite" received this name due to their sophisticated and

exceptional hacking talents (Holt 2010, Jordan & Taylor, 1998, Taylor 1999).

Similarly, Rogers (2006) created a preliminary taxonomy based on motivation

and skill level to classify computer criminals into nine groups. The nine categories are

listed and described bellow (Rogers, 2006):

1. Novice (NV) – This group refers to individuals with very little
   knowledge of hacking and to engage in hacking behaviors and attacks
   these individuals need pre-written tools or scripts from more advanced
   hackers. This is the lowest level of skills out of the 9 groups.

2. Cyber Punks (CP) – This group refers to individuals with more
   computer knowledge than the NV group and usually posses some
   programming skills and therefore is able to write basic level scripts.
   These individuals also have a better understanding of the systems they
   are attacking and attack with malicious intent.

3. Internals (IN) – This group of individuals usually posses a greater skill
   set do to their IT positions and are typically disgruntled employees
   who abuse the amount of trust their position is given.

4. Petty Thieves (PT) – This group of individuals has moved toward
   using technology to facilitate a crime because their target has moved in

this direction (Ex. banks). Typically this group is motivated by financial gain and greed.

5. Virus Writers – this category is an example of the sub-groups within hacking classifications and research suggests individuals grow out of this stage

6. Old Guard Hackers (OG) – This group is motivated by an intellectual challenge and curiosity, often writing a script with no intent to use it but these individuals do post the script online and thus lower level hackers can use the script.

7. Professional Criminals (PC) – similar to traditional crime, these individuals are motivated by financial gain. They use their technical skills to further then criminal endeavors.

8. Information Warriors (IW) – This group refers to individuals who job is to protect and defend various types of computer systems. Typically this group of individuals is highly trained and motivated.

9. Political Activist (PA) – included in this specific model as a place holder to balance out the categories; typically refers to hackers with a political agenda

Lastly, hackers may be classified based on their position within or outside a company. Those who work within a company or government agency who attack the network/infrastructure are considered "insiders" while those who are not employed by a company or agency are considered "outsider". Contrary to some beliefs, researchers have

shown that a large amount of attacks actually come from trusted individuals within a company or government agencies (Shaw et al., 1999).

2.2.2   History

The Internet refers to the "global communication network that allows almost all computers worldwide to connect and exchange information" (Meeriam-websiter). In 1969, the Advance Project Research Agency Network (APRAnet) was responsible for the first group of computers communicating with one another (Elon). In 1970, there were only 100,000 computers in use in the United States (Schell, 2007). In 1989, British scientist Tim Berners-Lee created the World Wide Web (WWW) and Hyper Text Transfer Protocol (HTTP) (CERN). The creation of HTTP and WWW allowed users to link information through Internet browsers and transfer information, changing the way individuals communicate. Statistics show a dramatic increase from 1998-200 in terms of homes with a computer and homes with Internet access, according to the United States Department of Commerce, Census Bureau. It should be notes that the Census did not start asking questions regarding owning of computers until 1984. The census Bureau found the percentage of homes with at least one individual who used the Internet to be up from 1998 (26%) to 2000 (42%), and more than doubled from 1997 (18%) to 2000 (Newburger, 2001). Additionally, in 1984, 8% of homes had a computer compared to 51% of homes in 2000 (Newburger, 2001). These statistics show a dramatic increase in less than 200 years, which researchers conclude that "the global shift in human behavior in a short time had direct ramifications for the threat posed by the malicious hacker community "(Holt & Schell, 2013; p. 6). Furthermore, Holt and Schell (2013) suggest

that since ARPnet was created over 40 years ago the world has become dependent on the

Internet.

<div align="center">2.3 <u>Profiling Computer Criminal: Introduction</u></div>

A vast amount of computer crime research focuses on understanding and

combating the technical aspect of digital forensics. However, researchers have suggested

computer crime and digital forensics is not only about the technology but also the

individuals involved in the criminal activity (Rogers et al., 2006; Furnell, 2002; Rogers &

Ogloff, 2003). Rogers and colleagues (2006) suggest the only way to combat the

phenomenon of computer crime is to focus on the people committing the crime.

Additionally, Crossler et al. (2012) argues future research needs to focus on gaining a

better understanding for different behavioral characteristics of hackers. Researchers are

unanimous in this need to better understand computer criminals, and this study aims to

add to the growing body of literature related to characteristics of computer criminals.

<div align="center">2.3.1 Computer Criminal Behavior Individual Differences</div>

To better understand computer crime, research looks at factors which might affect a

person's criminal computer behavior. Rogers, Smoak and Liu (2006) examined motives

and personality characteristics of individuals who engage in computer related crime.

Respondents reported their criminal computer activity through the Computer Crime Index

(CCI; Rogers et al., 2006). Results from this portion of the survey indicate 38.3% of

respondents had committed at least one of the incidents measured in the past three years

(Rogers et al., 2006). From the list of computer-related crimes, the most frequently

reported was guessing another's password (87%; Rogers, Smoak & Liu, 2006).

Additionally, individuals who reported computer-related deviant behavior scored

significantly lower on the Moral Choice Internal and Moral Choice Social compared to participants that reported no computer-related deviant behavior (Rogers, Smoak & Liu, 2006). The group consisting of individuals who reported computer deviant behavior scored high on exploitive manipulative amoral dishonesty (Rogers, Smoak & Liu, 2006).

Rogers, Seigfried and Tidke (2006) also examined self-reported computer criminal behavior among undergraduate students enrolled in an information technology course. 88% percent of students were classified as computer criminals (Rogers, Seigfried, & Tidke, 2006). If the participant indicated that they guessed a password, used another person's password without authorization, looked at another's files without authorization, changed another's files without authorization, used or wrote a virus, obtained someone else's credit information without authorization, or used a device to obtain free phone calls, the individual was classified as a computer criminal (Rogers, Seigfried, & Tidke, 2006). Rogers and colleagues (2006) found extroversion to be the only predicting factor for computer criminal behavior; the authors also examined exploitive and manipulative behavior but found no difference between self-reported computer criminals and non-computer criminals in terms of these behaviors (Rogers, Seigfried, & Tidke, 2006). These findings are contradictory to a similar study conducted by Rogers, Smoak & Liu (2006). In addition, Rogers, Seigfried, and Tidke (2006) found that moral reasoning was not significantly correlated with criminal computer behavior, which also opposed previous findings from Rogers, Smoak & Liu (2006). Rogers, Seigfried, and Tidke (2006) suggest the reason for the mixed results may be due to Rogers, Smoak, and Liu's (2006) sample; participants were from a liberal arts university in Canada.

A more recent study by Seigfried-Spellar and Treadway (2014), examined deviant computer behavior and non-deviant computer behavior among college students based on college major. This study aimed to determine if degree major or minor had a relationship to deviant or non-deviant online behavior among undergraduate students. The study also looked at individual differences to see if participants who engaged in deviant or non-deviant computer behavior could be distinguished by personality traits. Seigfried-Spellar and Treadway (2014) surveyed a large, southern university, resulting in a sample size of 398 undergraduate students who voluntarily completed the online survey. The study's results included a few significant differences in personality traits between self-reported computer deviants and non-deviants. Overall, hackers majoring in the arts were more extraverted than those majoring in both the arts and business, and virus writers were more antagonistic, more likely to exhibit constraint, and less likely to follow social norms or make decisions based on morals (Seigfried-Spellar & Treadway, 2014).

Additionally, research has examined what primary factors contribute to young individuals with computer talent becoming hackers (Hu, Zhang, & Xu, 2012). The first predicting factor was the number of hours a student spent playing online computer games versus engaging in sports activities outside (Hu, Zhang, & Xu, 2012). Results indicated participants who spent more hours engaged in online games were more likely to partake in hacking activities, whereas spending time playing sports outside served as a counter activity to behaviors (Hu, Zhang, & Xu, 2012). Secondly, morality played a role in predicating hacking behaviors. Specifically, Hu and colleagues (2012) found the more participants believed hacking was morally wrong, the less likely they were to engage in such behavior. The authors suggest morality may be the number one weapon in fighting

against computer hacking (Hu, Zhang, & Xu, 2012). The final predicting factor measured for hacking behaviors was self-control. Results showed the "temper dimension of self-control has a strong and positive effect on the likelihood of hacking" (Hu, Zhang, & Xu, 2012, p. 3067). Participants who became easily irritated and angry were more likely to engage in hacking activates (Hu, Zhang, & Xu, 2012). Overall, Hu, Zhang, and Xu (2012) found moral beliefs, self-control, and time spent on computer games versus outdoor sport activities were predicting factors for hacking behaviors.

Some aspects of the Internet can be completely anonymous, resulting in individuals believing it is a good environment in which to conduct criminal activity (Selywn, 2008) Selwyn (2008) concluded undergraduates view the Internet as a safe place to misbehave, as 93.9% of respondents reported engaging in at least one of the following online behaviors within the past month: misrepresentation of self, unauthorized use of another's account, plagiarism of an essay or assignment, unauthorized downloading of music or film, and pornography use. More specifically, 51% of respondents reported misrepresenting themselves online, 26% reported the unauthorized use of another's account, and 40% indicated the use of pornography (Selwyn, 2008). These statistics also draw attention to the prevalence of deviant behaviors among college students.

2.4   Addiction: Introduction

As previously stated from Hu, Zhang and Xu (2012) study, the number of hours an individual spends partaking in computer games highly predicts their likelihood to engage in hacking behaviors compared to individuals who spend more hours engaging in outdoor sports activities. These findings suggest that individuals who are spending more

time on the computer, playing video games, are more likely to participate in computer hacking. Based on the findings of Hu, Zhang amd Xu (2012), research should examine the relationship between time spent online the relationship it has to computer deviant behavior. Therefore, this study aims to examine the relationship between internet addictive behaviors and computer deviant behavior. To begin the literature on internet addiction, it is imperative to first understand the definition and characteristics associated with *general* addiction.

2.4.1   Defining Addiction

Based on popular notions, addiction has come to refer to over using alcohol and drugs. However, originally, addiction simply meant "giving over" or being "highly devoted" to a person or thing (Alexander, & Schweighofer, 1988). Additionally, the term originally referred to engaging in a behavior habitually, which could have a positive or negative effect (Levine, 1978). The Oxford dictionary defines addiction as "the fact or condition of being addicted to a particular substance, thing, or activity"(Oxford, 2015). The oxford dictionary definition of addiction recognizes that addiction can refer to not only a substance, but also things and activities. However, Goodman (1990) draws attention to the fact that psychiatrist and psychologist typically focus their attention on mental / behavior disorders in terms of therapy and theory related to addiction. According to Sussman & Sussman (2011) the following five characteristics comprise addiction: feeling different, temporary satiation, preoccupation with the behavior, loss of control and negative consequences. In addition, two hallmarks of addiction include tolerance and withdrawal (Sussman & Sussman, 2011).

2.4.2 Case Study: Gambling and Addiction

For a complete understanding of addiction, it is important to also look at the evolution of addiction and the behaviors that fall into the category of addiction. In the British Journal of Addiction, Goodman (1990) compares the Addictive Disorder criteria with the Pathological Gambling criteria. In the third addition of the *Diagnostic and Statistical Manual of Mental Disorders* (DSM) the following is the criteria for an Addictive Disorder:

A. Recurrent failure to resist impulses to engage in a specified behavior

B. Increasing sense of tension immediately prior to initiation the behavior

C. Pleasure or relief at the time of engaging in the behavior

D. A feeling of lack of control while engaging in the behavior

E. At least three of the following:

1. Substance often taken in larger amounts or over a longer period than the person intended

2. Persistent desire or one or more unsuccessful efforts to cut down or control substance use

3. A great deal of time spent in actives necessary to get the substance (theft) taking the substance (chain smoking) or recovering for its effects

4. Frequent intoxication or withdrawal symptoms when expect to fulfill major role obligations at work, school or home (e.g. does not go to work because hung over, goes to school work "high", intoxicated while taking care of his or her children) or when the substance is psychically hazardous (e.g. drives when intoxicated)

5. Important social, occupation or recreation activities given up or reduced because of substance use

6. Continued substance use despite knowledge of having a persistent or recurrent social, psychological or physical problem that is cause or exacerbated but the use of substance (e.g., keeps using heroin despite family arguments about it, cocaine-induced depress, or having an ulcer made worse by drinking)

7. Marked tolerance: need for markedly increased amount of substance (i.e., at least 50% increase) in order to achieve intoxication or desired effect, or markedly dismissed effect with continued use of the same among

8. Characterizes withdrawal symptoms

9. Substance often taken to relieve or avoid withdrawal symptoms

F. Some symptoms of the disturbance have persisted for at least 1 month, or have occurred repeatedly over a longer period of time.

Since this list was comprised in the 3rd addition of the DSM two more additions have been published. However, for this case study it is important that to look at the original list of criteria used in the Goodman (1990) comparison of addiction and gambling. The criteria for Pathological Gambling include:

Maladaptive gambling behavior, as indicated by at least four of the following:

1. Frequent preoccupation with gambling or with obtaining money to gambling

2. Frequent gambling or larger amounts of money or over a longer period of time than intended

3. A need to increase the size of frequency of bets to achieve the desired excitement

4. Restlessness or irritability if unable to gamble

5. Repeated loss of money by gambling and retuning another day to win back loses ('chasing')

6. Repeated efforts to reduce or stop gambling

7. Frequent gambling when expect to meet social or occupation obligations

8. Sacrifice of some important social occupation or recreation activity in order to gamble

9. Continuation of gambling despite inability to pay mounting debts, or despite other significant social, occupation or legal problems that the person knows to be exacerbated by gambling

When comparing these lists, and also pointed out by Goodman (1990), there are many similarities between the two. Goodman (1990) points out the following comparisons (p. 1405):

" (1) of Pathological Gambling correspons to (1) of Addictive Diesorder,(2) to (2),(3)to (8), (4) to (9), (6) to (3), (7) to (5), (8) to (6), and (9) to (7)."

As Goodman (1990) draws attention to, the DSM-III criteria and the pathological gambling criteria are remarkably similar. Almost 15 years after Goodman's 1990 article, the 5th edition of the DSM was published, which has significant differences compared to DSM-III. The DSM-V important change, for the purpose of this case study, included the addition of Gambling Disorder in this chapter on addiction. Rogers Hosptial, which is a

leader in comprehensive and effective behavioral health care treatment for children, teens and adults, described the key changes in the DSM-5. The addiction chapter in the DSM-5 has usually focused on disorders involving substance use, using terms like abuse and dependence (Rogers Hospital, 2014). However, now, the chapter includes gambling disorder and the terminology "addiction" (Rogers Hospital, 2014). In a press release from Rogers Hospital (2014) on the new changes to the DSM-5 the following quote appeared: "change within the DSM reflects increasing evidence that some behaviors – like gambling – can activate the brain reward system with effects that are similar to those of drug use". It is estimated that 2-3% of Americans suffer from gambling addiction.

This literature presented is not aiming to argue whether or not Internet addiction is fact or fiction but, rather provide evidence that addiction does not only apply to substances but also behaviors. Truan (1993) noted people are said to be "addicted" to food, smoking, gambling, shopping, work, play and sex. The American Psychology Association and DSM-5 currently does not recognize or include internet addiction when discussing addictions. However, addictive behaviors, such as gambling, have become more recognized in recent years.

2.5   Internet Addiction: Definition and Characteristics

For the purpose of this study int111ernet addiction is used a predictive variable for computer deviant behavior. Although the DSM-V does not recognize Internet Addiction as a current addiction, a substantial amount of empirical research has been conducted examining characteristics of Internet Addiction. Traditionally addiction has referred to a physical dependence on a substance (Holden, 2001), however recently addiction has been applied to excessive use of the Internet. Internet Addiction has been defined as

problematic, excessive, or mal-adaptive use of the Internet (Thombs, 1994; Young, 1998). Griffiths (1999) list the following six components of internet addiction (p. 246-247):

1. Salience – the activity of being online becomes the most important aspect of an individual's life.

2. Mood Modification – Individuals get an "arousal" or "buz" for logging on to the Internet.

3. Tolerance – Individual's have to increase the amount of time spent on the Internet to experience a mood modification

4. Withdrawal Symptoms – Individual's may experience withdrawal symptoms (e.g., moodiness) when unable to long on to the Internet.

5. Conflict – Individual's experience conflicts with other's as a result of their Internet use.

6. Relapse – Individual's revert back to old tendencies of Internet use after attempting to change the behavior.

Griffiths (1999) components for Internet Addiction are similar to Sussman & Sussman (2001) and the DSM III list of attributes of addiction. Withdraw symptoms and tolerance are seen as the hallmark of substance abuse and addiction (Sussman & Sussman, 2001). Similarly, according to Marks (1990) behavioral addiction characteristics share similar attributes with substance abuse. Mark (1990) specifics the following similarities (p. 1391):

Common across dependence syndromes is: a repeated urge to engage in behavior known to be counterproductive; mounting tension until it is completed; rapid temporary switching off of the tension by completing the behaviour; gradual

return of the urge; syndrome-specific external and perhaps internal cues for the

urge; secondary conditioning of the urge to external and internal cues; similar

strategies for relapse prevention by cue exposure and stimulus control. The urge

to complete a behavior and discomfort if prevented from this resemble the craving

and the withdrawal (WD) symptoms of substance abusers.

Based on the Griffiths (1999) components of Internet Addiction and Marks (1990)

description of behavioral addiction, researchers suggest Internet addiction fits the

attributes of behavioral addictions.

<div align="center">2.6   <u>Internet Addiction Research and Instruments</u></div>

Due to groundbreaking research, research has credited Kimberly Young's

research with making Internet Addiction Disorder popular (Douglas et al., 2008, p. 3029)

Young (1998) created an eight-item Diagnostic Questionnaire (DQ) with modified

criteria for pathological gambling. Results indicated the majority of responders were

Internet dependents (396) compared to non-dependent Internet respondents (100)

(Youngs, 1998) Young (1999) lists 8 characteristics of Internet Addiction and users must

exhibit 5 or more attributes. The list consists of the following 8 characteristics (Young,

1999):

1. Individual is preoccupied with the Internet

2. Individual needs longer amounts of time on the Internet

3. Individual continues to attempt to limit Internet use

4. Individual experiences withdrawal symptoms when reducing Internet use

5. Time management issues are experienced by the Individual

6. Individual experiences environmental distress (individual family, school, works, etc)

7. Individual experiences deception about time related time spent online

8. Mood modification through Internet use

Young & Rodgers (1998) examined personality traits associated with Internet Addiction. Results from 259 cases of dependent Internet use revealed dependents scored high on self-reliance, emotional sensitivity and rapacity, vigilance, low self-disclosure and non-conformist personality traits (Young & Rodger, 1998).

Results from a survey of 563 participants indicate the average respondent spent an average of 19 hours on the Internet per week and experienced at least 10 signs of problems due to their Internet use, such as failures to manage time, missing meals, etc (Brenner, 1997). Brenner (1997) also found evidence of tolerance (55%), withdrawal (finding it hard to stop using the internet, 28%), and craving (trying to spend less time on the internet, 22%). Additionally, Leung (2004) conducted a study focusing on the Net-generation, children of the baby boomers, and internet addiction. Results from Leung (2004) indicated Net-geners addicted to the Internet tend to be young female students. Additionally, problematic internet use was associated with emotionally openness to the Net and heavy use of ICQ. Comparable to Leung (2004), Anderson (2010) found student use the Internet for an average of 100 minutes per day and these individuals were significantly more likely to encounter negative effects on their sleep pattern, academic work and meeting new people. Of the 1,078 Internet users in Andersons (2010) study, 106 reported matching criteria for Internet dependence.

2.7   Internet use, addiction and computer deviance

Research has begun examining the relationship between internet use, addiction and various computer deviant behaviors. For instance, a study conducted by Eksi (2012) examined narcissistic personality traits' predicting levels of Internet addiction and cyber bullying. Results indicated the variable that significantly predicted cyber bullying was the sub-dimension of internet addiction, social isolation. Additionally, Hinduja and Patchin (2008) found computer proficiency and time spent on-line were related to both victim and offenders of cyber bullying.

2.8   Computer Use and Literacy of College Students

According to Junco et al. (2007), anyone born since 1983 is considered to be part of the "net generation." Since the turn of the millennium, the net generation has been entering college, meaning the current student population is comprised solely of this technologically proficient group of individuals. According to Junco and colleagues (2007), "the 'net generation' is the most technologically advanced group of students to ever enter into college" (p. 33). Empirical research has looked at the prevalence of computer usage among college students; this research will be discussed next.

2.8.1   Computer Use

The Pew Internet and American Life Project conducted a study throughout 2010 which examined technology use among students. The study specifically examined participants who reported attending community college, four-year universities, and graduate programs. In terms of general Internet use, findings suggest young adults are more likely to go online when compared to the general population (Smith et al., 2011). More specifically, 92% of adults ranging between 18 to 24 years of age who do not

attend college use the Internet, compared to nearly 100% of undergraduate and graduate

level college students who use the Internet (Smith et al., 2011). Specifically regarding

home broadband access, 95% of undergraduate students and 93% of graduate students

can access the Internet from their homes (Smith et al., 2011). These statistics are well

above the national average, which is 65% for adults (Smith et al., 2011). Additionally,

Smith et al. (2011), found a significant difference between those who owned computers

and those who owned laptops; 60% of adult respondents owned a desktop computer,

compared to 73% of graduate level students (Smith et al., 2011). Similarly, 52% of adults

owned a personal laptop, which is substantially lower than the 88% of undergraduate

students and 93% of graduate students. The Smith et al. (2011) study shows the

prevalence of Internet usage is extremely high among young adults, more specifically

undergraduate and graduate students.

Additionally, empirical research has been conducted looking at Internet and

computer usage, specifically among undergraduates. Anderson (2001) found that, among

1,302 undergraduates surveyed, the average amount of time spent using the Internet was

100 minutes per day. Similarly Jones, Johnson-Yale, Millermair, and Perez (2009) found

66% of male and 56% of female college students sampled have more than 10 years of

experience using the Internet; 50% of males and 33% of females reported spending more

than three hours per day using the Internet. In addition, 26% of students sampled

reported using the Internet for two to three hours a day, whereas 36% of females and 19%

of males reported using the Internet for just two hours or less per day (Jones et al., 2009).

2.9   <u>Summary</u>

With the constant growth of computer related crime coupled with the rapid proliferation of the globalization of technology, the need to better understand these types of criminals is imperative. Empirical research aims to determine behavioral characteristics that predict deviant computer behavior. A review of the literature provides evidence of various characteristics related to computer deviant behavior, such as: college major, personality characteristics, time spent online and morality. In addition, the literature review provided an overview of Internet addiction research. The current study aims to fill the gap in the literature by directly examining the characteristics of Internet addiction relationship to computer deviant behavior. The research methods associated with the current are discussed next.

CHAPTER 3. METHODOLOGY

3.1   <u>Hypothesis</u>

Based on the literature review, the following five hypotheses were tested; specifically, regarding internet addiction and computer deviant behavior the following two hypotheses will be tested:

H.1. Time spent online will be correlated with computer criminal behavior

H.2. Characteristics related to Internet addiction will be more common among students who are classified as computer criminals.

Based on previous studies regarding personality characteristics of computer deviants, the following three hypotheses will be tested:

H3. Extraversion will be a significant factor when predicting criminal computer behavior of college students.

H.4. Manipulative / exploitive behavior will be higher among college students who are classified as computer deviant.

H.5. Moral reasoning scores will be different between participants classified as computer deviants and those not classified as computer non-deviant.

<center>3.2   <u>Sample</u></center>

Participants were voluntarily recruited using a snowball sampling method via the Internet. Snowball sampling refers to a "non-probability sample where people who are part of the sample are asked to refer other people to also participate in the study" (Donley, 2012). The survey was E-mailed to professors/instructors at multiple universities and the solicitation e-mail asked the professor/instructors to pass the survey along to their students as well as any other professors who would be willing to also send out the survey. Similarly, the solicitation e-mail for the students asked them to invite their friends/classmates to participate in the survey. Additionally the survey was advertised on various social media sites, including Facebook and Twitter, in which the research will asked individuals to partake in the survey and also ask their friends and family to as well. The method, similar to a snowball, is thought to get bigger over time based on individuals recruiting others. Snowball sampling is also an appropriate method to use when asking participants about their engagement in illegal activity (i.e., illegal computer criminal behavior), according to Donley (2012). Furthermore, Donley (2012), gives an example of an appropriate instance for using snowball sampling, which is similar to the current study:

> Let's suppose a research wants to study computer hackers. The research knows two people that engage in this activity. He asks both of them to participate in the research and they agree. He then asks them if they can refer other hackers to participate in the study. They each know two more people that are hackers. (p. 98)

The current study sampled college students (both bachelorette (undergraduate) and graduate level). Specifically, the current study aimed at sampling the "net"generation. The literature shows college students spend an overwhelming amount of time online (Anderson, 2001; Jones et al., 2009; Smith et al., 2011), therefore this demographic would serve as an appropriate sample for examining personality differences between non-deviant and deviant computer behavior. Participants were required to currently be enrolled in college (undergraduate or graduate level) to participate in the study as well as over the age of 18 years old, which is the age of consent in the United States. In addition, the survey was only offered in English and therefore respondents were required to be able to read the English language.

3.3   Survey Design

The survey was created using an online platform, Qualtrics, which is a research-based survey website. Lewis and colleagues (2009) found web-based survey generated a more diverse sample based on demographics for both age and gender. Also, the web-based survey produced a more gereralizable sample (Lewis et al., 2009). The online questionnaire began by requesting basic demographic information, such as sex, age, and geographical locations. The demographic questions were placed first for two important reasons. First, the question asked participants to indicate their age, if the respondent is not 18 years or older they are not allowed to participate in the survey. Second, the demographics are essential to this study for comparison and descriptive purposes. Research has shown that respondents often drop out of surveys prior to completing the survey entirely (Teclaw, Price & Ostuke, 2012), therefore putting the demographic questions first was imperative. Additionally, Teclaw, Price & Ostuke (2012) found

placing demographic questions at the front of the survey increased item response rate for the demographic section. Research has also found the forward placement of the demographic questions had no affect for item responses for non-demographic questions or the average mean score (Teclaw, Price & Ostuke, 2012). Portions of the survey asked respondent to indicate their involvement in various types of computer criminal behavior and therefore it was imperative to put the demographic questions first in effort to limit lying on the demographic questions.

After these initial queries, the participants answered 5 different Likert scale questionnaires pertaining to their deviant computer-related activities, personality characteristics, and Internet addiction. These 4 questionnaires were found to be reliable in previous research (Rogers et al., 2006a; Rogers et al., 2006b). The first questionnaire comprised of the Computer Crime Index-Revised (CCI-R; Rogers, 2001), consisting of a five-point Likert Scale. The CCI-R measures the frequency of self-reported deviant computer activity, how often participants engaged in deviant computer activity within the last 3years, and how old participants when they first engaged in deviant computer behavior (e.g., virus wringing, obtaining passwords, etc.).The author removed one question from the CCI-R, which asked participants if they ever "knowingly used, made or gave to another person a device to obtain free long distance phone calls," because this technique, known as phone phreaking, is no longer in practice due to new technology. The CCI-R comprised of three groups of questions, with 22 questions in each section; the three groups consisted of the same 22 questions and the only thing which changed was the directions and likert-scale choices. For example, participants were asked if they have if they have ever tried to guess another's password to get into his/her computer account

or files without permission; on the first question set, the choices asked participants to indicated when the last time they engaged in this activity; the second set asked how often in the last three years they engaged in the activity and the last set asks what age the participant was when they first engaged in the activity. Based on item response to the CCI-R, was treated as a dichotomous variable was created Computer Deviant (0) versus Computer non-deviant (1).

Secondly, the Big Five personality traits were assessed usimg Goldenberg (1992) scale. Respondents were tasked with answering questions pertaining to their personality traits. Specifically, agreeableness, conscientiousness, neuroticism, extraversion, and openness to experience will be measured. Participants were given a set of two words and asked to pick which word they identify with the most. The calculated Cronbach's alpha for the current study subscales were: extraversion = 0.91, agreeableness = 0.91, conscientiousness = 0.92, neuroticism = 0.88, and openness to experience = 0.92.

The third portion of the survey consisted of the Exploitive Manipulative Amoral Dishonesty Scale, with a nine-point Likert scale, ranging from "strongly disagree" to "strongly agree" (EMAD; Altemeyer, 1995). The EMAD scale measured the degree of exploitive and manipulative traits an individual possess. Forth, participants completed the Moral Decision Making Scale (MDKS: Hldkyj, 2002). The MDKS measures participants' moral decision making by using the following three subscales: internal, social, and hedonistic. Example from the MDKS portion of the survey includes "whether my choice hurts or benefits others". The calculated Cronbach's alpha from the current study for the MDKS subscales were internal = 0.88, social = 0.55 and hedonistic = 0.73.

Finally, participants answered questions from Internet Addiction Survey. The survey was comprised of 20 questions and respondents were asked to rate their answer on a five-point Likert scale ranging from 0=Not Applicable 1=Rarely 2=Occasionally 3=Frequently 4=Often 5=Always (Young & Abreu, 2010). Questions asked respondents about problematic internet use, for instance: "How often do you find that you stay online longer than you intended?" The results based on the five-point Likert scale are calculated, the higher the score indicates are a greater level of addiction. The following scale is suggested for grouping calculated scores: Normal Range: 0–30 points; Mild: 31–49 points; Moderate: 50–79 points; Severe: 80–100 points (Young & Abreu, 2010). The Internet Addiction Test (IAT) was the first validated instrument to access Internet Addiction and is widely used. (Widyanto&McMurren,2004). The calculated Cronbach's alpha for the IAT questionnaire was 0.93. The survey took approximately 15 minutes to complete.

3.4   Procedure

The survey was administered electronically using an anonymous, Internet-based survey on Qualtrics .Qualtrics assigns an identification number to each participant instead of collecting Internet Protocol (IP) information. This feature prevented any identification of the respondents to be reordered by the program or the researchers, which increases the confidentiality of the respondents. The researcher did not have any face-to-face contact with the respondent however; it will be possible for respondent to contact to the research by phone or e-mail. In accordance with the Institutional Review Board (IRB), respondents are given the contact information of the research for the purpose of asking questions regarding the study. Additionally, Qualtrics [has] various features that allow for

easy execution of Likert scales, consent forms, and forced responses. Force response is necessary for the first question of the survey, which asks respondent to indicate their age in years. By utilizing the force response option in Qualtrics the researcher was able to only allow individuals indicating they are 18 years of age or older to continue with the survey.

The study was advertised to students through e-mail. McGraw, Tew and Williams (2000) found the Internet is "adequate to permit Web delivery of many cognitive and social psychological experiments" (p. 502). Respondents were not compensated for their participation. Upon accessing the website, the homepage explained the nature of the study and also act as a consent form to which the respondent will have the option to either agree or decline to participate in the current study, per IRB protocols. The consent page detailed that the survey is completely voluntary and assure the confidentiality of the data collected. To participate in the study, respondents were asked to indicate their age. If potential respondents did not meet the age requirement (18 years of age, per federal guidelines regarding an individual's age of majority), they were immediately directed to the "Thank You" page of the survey and disallowed from continuing the survey. If participants met the age requirement and agree to take part in the survey (i.e., by clicking the "I Agree" button at the bottom of the consent page), they were granted access to continue with the remaining sections of the survey.

The study took approximately 15 minutes to complete, and during the course of the survey, absolutely no identifying information was collected (e.g., name, social security number, IP address); instead, participants were randomly assigned an ID number. Anonymity and confidentiality is important in order to increase the participant's

confidence in self-disclosing potentially illegal computer activity. In addition,

participants were able to quit the survey at any time with no ramifications, and contact

information for the investigator conducting the survey was be provided

3.5   Statistical Analysis

For the statistical analysis the author will use SPSS. Prior to analysis, significant

was set. Specifically, regarding each hypothesis, the following significance levels were

set:

H.1. Time spent online will be correlated with computer deviants behavior; one-
tailed   statistical significance with the alpha level of 0.02

H.2. Characteristics related to Internet addiction will be more common among
students who are classified as computer deviants; one-tailed statistical
significance with the alpha level of 0.02

H3. Extraversion will be a significant factor when predicting criminal computer
behavior of college students; two-tailed statistical significance with the alpha
level of 0.05

H.4. Manipulative / exploitive behavior will be higher among college students
who are classified as computer deviant.; one-tailed statistical significance with the
alpha level of 0.02

H.5. Moral reasoning scores will be different between participants classified as
computer deviants and those not classified as computer non-deviant; one-tailed `
statistical significance with the alpha level of 0.02

Additionally, prior to analysis the raw data was examined for missing information.

Participants which did not give consent, were not classified as students and who did not

complete the survey entirely were removed from the final data set. Frequency analyses were conducted to determine the demographic information of the participants. Next, a zero-order correlation was conducted to identify any personality characteristics that are significantly associated with the various computer crime classifications. Then, the characteristics significantly related to computer criminal behavior were entered into a logistic regression (LR). Researchers Tabachnick & Fidell (2007) suggest Logistic regressions (LG) are appropriate for this type of data because LR violate fewer assumptions than other analysis and are more robust.

The results will be discussed in two main sections: descriptive and research question/ hypothesis testing. The descriptive section will detail the sample size, final data set and demographic information for the respondents. Next, the results from the hypothesis testing will be discussed.

3.5.1   Operational Definition of Construct

In order to define the dependent and independent variables inherit to this study, it is important to first look at the research question for the current study: does the Rogers, Siegfried, Tidke model and internet addiction predict self-reported computer criminal behavior among college students? The Rogers, Siegfried, Tidke model, as previously mentioned in the literature, refers to a survey consisting of the CCI-R, Big-5, EMAD and MDKS. The current study defined the independent and dependent variable as follows:

> Dependent: Respondents' answers regarding cybercriminal behavior will be used as a grouping variable (independent variable). Previous research has categorized respondents based on their involvement in computer deviant behavior

Independent: extraversion, openness to experiences, agreeableness, conscientiousness, neuroticism, moral choice hedonistic, moral choice internal, and moral choice social, exploitive behavior, manipulative behavior and internet addiction scores.

3.6   Summary

In summary, the current study used a snowball sampling method via the Internet to generate a sample of college students, both undergraduate and graduate level. The online survey was comprised of demographics, CCI-R, Big5, EMAD, MDKS and Internet Addiction Scale and took approximated 15-20 minutes to complete. Only individuals who were 18 years or older were allowed to voluntarily participate in the survey and consent was necessary for participation. Statistically analysis were conducted examining the dependent (predictive) group variable, computer criminal (1) versus non-computer criminal (0) and the 10 independent variables (extraversion, openness to experiences, agreeableness, conscientiousness, neuroticism, moral choice hedonistic, moral choice internal, and moral choice social, exploitive behavior, manipulative behavior and internet addiction scores). The next chapter details the statistical results from the current study.

CHAPTER 4. RESULTS

Prior to analysis, statistical significance was set. Frequency analyses were run to determine the demographics of respondents, including gender, race, college classification, etc, as well as technology ownership and use. Next, a zero-order correlation was conducted to determine if any of the independent variables (predictors) were significantly related to the dependent variable, computer behavior. The independent variables included answers from the Goldberg's Modified Big 5 Personality Questionnaire (Big5), Moral Decision Making Scale (MDKS), Exploitive Manipulative Amoral Dishonesty Scale (EMAD) and Internet Addiction Test (IAT). After finding relationships between the independent and dependent variables, a one-way analysis of variance (ANOVA) was conducted, which further confirmed the significant findings from the zero-order correlation. Variables which were found significant in both the zero-order correlation and ANOVA were then entered into a logistic regression to determine the best predictive model.

4.1   Data Exploration

The raw data set included 169 respondents; after initial examination 64 (38%) respondents were eliminated because of missing data / unfinished questions. Additionally, three (1.7%) respondents did not provide consent and six (3.5%) respondents were not students and therefore not included in the final data set.

Next the researcher put the respondents into grouping variables based on their answers to the Computer Crime Index-Revised (CCI-R), which resulted in a dichotomous variable of computer non-deviant (0) and computer deviant (1). Due to in-consistent answers across the three scales of the CCI-R, one (0.5%) respondent was eliminated. The final data set included 95 respondents, 49 (52%) computer deviants and 46 (48%) computer non-deviants

As shown in Table 1, the majority of the sample ($n = 95$) were female (63%), single/never married (83%), heterosexual (90%) and Caucasian (83%) and ages range between 18 to 21years of age (43%) Additionally, the majority comprised of graduate level college students (38%) and nearly half attended a college in the state of Indiana (46%).

41

Table 4.1 Demographics of Computer Deviants and Computer Non-Deviants

| Variable | | Computer | | |
		Deviant (*n*=49)	Non- Deviant (*n*=46)	Total (*n*=95)
Sex	Male	19 (39%)	16 (35%)	35(37%)
	Female	30 (61%)	30 (65%)	60 (63%)
Age	18-21	23(47%)	18(39%)	41(43%)
	22-25	14(28%)	11(24%)	25(27%)
	26-30	7(14%)	8(17%)	15(16%)
	31-39	3(6%)	5(11%)	8(8%)
	>40	2(4%)	4(9%)	6(6%)
College Classification	Freshman	8 (17%)	9 (19.5%)	17 (18%)
	Sophomore	3 (6%)	7 (15%)	10 (10%)
	Junior	10 (20%)	5 (11%)	15 (16%)
	Senior	7(14%)	9 (19.5%)	16 (17%)
	Graduate	20 (41%)	16(35%)	36 (38%)
	Other	1 (2%)	0	1(1%)
State	Alabama	5(10%)	4(9%)	9(10%)
	Florida	9(18%)	10(22%)	19(20%)
	Indiana	26(54%)	18(39%)	44(46%)
	Other	9(18%)	14(30%)	23(24%)
Race/Ethnicity	Asian	2(4%)	5(11%)	7 (7%)
	Caucasian / White	43(88%)	36 (78%)	79 (83%)
	Other	4(8%)	5 (11%)	9 (10%)
Marital Status	Single, never married	43 (88%)	36 (78%)	79 (83%)
	Married	5 (10%)	9 (20%)	14 (15%)
	Divorced	1 (2%)	1 (2%)	2 (2%)
Sexual Orientation	Heterosexual	46 (94%)	39 (85%)	85 (90%)
	Homosexual	2 (4%)	2 (4%)	4 (4%)
	Bi-Sexual	1 (2%)	1 (2%)	2 (2%)
	Prefer not to respond	0	4 (9%)	4 (4%)

Note. Values represent frequencies with percentages in parentheses.

As shown in Table 2, the majority those who self-reported as being computer deviant own a personal computer (100%), use their computer daily (94%), own a cell phone (100%) and use their cell phone multiple times a day (61%). In addition, 90% of computer deviants have an active Facebook account and 63% have an active twitter account.

Table 4.2 Computer Deviants and Computer Non-Deviants Computer Use and Ownership

Variable		Computer		Total
		Deviant (n=49)	Non- Deviant (n=46)	Total (n=95)
Computer Own	Yes	49(100%)	45(98%)	94(99%)
	No	0	1(2%)	1(1%)
Computer Use	Daily	46(94%)	42(92%)	88(93%)
	Weekly	2(4%)	1(2%)	3(3%)
	Monthly	1(2%)	2(4%)	3(3%)
	Never	0	1(2%)	1(1%)
Own Cell Phone	Yes	49(100%)	45(98%)	94(99%)
	No	0	1(2%)	1(1%)
Cell Use	Once a day	0	2(4%)	2(2%)
	Multiple times a day	19(61%)	23(50%)	42(44%)
	Most of the day	30(39%)	20(44%)	50(53%)
	Never	0	1(2%)	1(1%)
Active Facebook Account	Yes	44(90%)	42(91%)	86(91%)
	No	5(10%)	4(9%)	9(9%)
Active Twitter Account	Yes	31(63%)	24(52%)	55(58%)
	No	18(37%)	22(48%)	40(42%)

Note. Values represent frequencies with percentages in parentheses

To determine which of the 10 independent variables had a significant relationship with computer behavior a zero-order correlation was conducted. Of the 10 independent variables, Internet addiction and openness to experiences were significantly correlated to computer criminal behavior, as shown in Table 3. Specifically, there was a significant positive relationship between self-reported computer behavior and Internet addiction characteristics, Pearson's Correlation Coefficient, $r_{pb} = 0.25$ ($p < 0.05$); $r^2 = 0.06$. Therefore, Internet Addiction accounted for 6.2% of variability in computer deviant and computer non-deviant score. Additionally, openness to experience was positively correlated with self-reported computer behavior, Pearson's Correlation Coefficient, $r_{pb} = 0.217$ ($p<0.05$); $r^2 = 0.047$; which indicates 4.7% is explained by computer behavior scores.

4.2   Hypothesis Testing

H.1. Time spent online will be correlated with computer deviants behavior.

Based on a zero-order correlation, there was no significant statistical evidence to support a correlation between computer deviant behavior and time spent online; $r_{pb} = 0.095$.

H.2. Characteristics related to Internet addiction will be more common among students who are classified as computer deviants.

Based on results from a forced entry logistic regression, statistical significance evidence indicated the higher the score on the Internet addiction test, the more likely you are to be classified as computer deviant; B = 0.04, Wald x^2 (1) = 4.39, $p < 0.05$, as show in Table 4. Specifically, you are 1X more likely to be a computer deviant if you score higher on the Internet addiction test.

H3. Extraversion will be a significant factor when predicting criminal computer behavior of college students; two-tailed statistical significance with the alpha level of 0.05

Based on results from zero-order correlation, there was no relationship between extraversion and computer criminal; Pearson's Correlation Coefficient. ; $r_{pb} = 0.171$, as shown in Table 3.

H.4. Manipulative / exploitive behavior will be higher among college students who are classified as computer deviant

Based on a zero-order correlation shown in Table 3, there was no relationship among manipulative / exploitive behavior and computer deviant behavior, Pearson's Correlation Coefficient, $r_{pb} = 0.142$.

H.5. Moral reasoning scores will be different between participants classified as computer deviants and those not classified as computer non-deviant

Statistical evidence reveled no significant relationships between moral reasoning scores and computer behavior based on a zero-order correlation, as shown in Table 3 (Social $r_{pb} = -0.046$ Internal $r_{pb} = 0.132$, Hedonistic $r_{pb} = 0.05$).

Table 4.3 Zero-Order Correlation between computer behavior and predicting variables.

					Predicting Variable					
	Comp Beh	IAT	Soc	Int	Hed	EMAD	O	N	C	A	E
Comp Beh	1	0.25*	-0.05	0.13	-0.05	0.14	0.22*	0.06	0.09	0.13	0.18
IAT		1	-0.16	-0.12	0.04	0.23*	0.17	-0.02	0.01	0.07	-0.10
Soc			1	0.61**	0.65**	-0.14	0.14	0.15	0.37**	0.27**	0.20
Int				1	0.67**	-0.04	0.29*	0.18	0.31**	0.34**	0.22**
Hed					1	0.03	0.22	0.11	0.26**	0.29**	0.06
EMAD						1	0.12	0.20	-0.04	0.01	-0.02
O							1	0.58**	0.76**	0.74**	0.49**
N								1	0.66**	0.70**	0.47**
C									1	0.78**	0.58**
A										1	0.62**
E											1

* p < 0.05 (2-tailed); ** p < 0.01 (2-tailed); *n* = 95

Note. IAT= Internate Addiction Test; EMAD = Emotional Manipulative Amoral Dishoensty; Soc = MDKS Social;

Int=MDKS Internal; Hed=MDKS Hedonistic; O=Openess; N=Neuroticism; C=Concisentiousness;

E=Extraversion; A=Agreeableness

Research Question

The research question for the current study is: Does the Rogers, Siegfried, Tidke model and Internet addiction predict self-reported computer criminal behavior among college students. Of the 10 possible variables to enter into the predictive model, based on the zero-order correlation, the only two independent variables related to computer behavior among college students is Internet Addiction, $F(1,93) = 6.17$, $p = 0.02$, and Openness to Experiences, $F(1,93) = 4.58$, $p = 0.04$. Based on the dependent binary grouping variable computer criminal (0) and non-computer criminal (1), a logistic regression (LG) was chosen to determine the best predictive model.

Overall, Internet Addiction and Openness to Experiences were significantly related to Computer Behavior, and therefore entered into the logistic regression predictive model. The enter method places all predictors into the regression model in one block and then parameter estimates are calculated for each block (Field, 2009). For the current study, the significant variables, Internet addiction and openness to experiences, were placed in the logistic regression. Results indicate Internet addiction is the best predictive variable for predicting computer behavior, Wald = 4.39, $p < 0.05$, as shown in Table 4. The model predicated 67% of computer deviants and 59% of non-computer deviants, for an overall success rate of 63%. The Hosmer and Lemeshow test was non-significant indicating the final model fit the data, $X^2 (8) = 6.39$ with $p = 0.60$.

Table 4.4 Summary of Logistic Regression for Computer Deviant Behavior

Variable	*B*	*SE B*	*Exp (B)*	*P*
IAT	0.04	0.20	1.04	0.04*
O	0.29	0.17	1.33	0.09

* p < 0.05

Note. IAT = Internet Addiction; O = Openness

4.4   Confirmatory Analysis

To further test the significant variables Internet Addiction and Openness to Experiences, which were found significant from the zero-order correlation, the research conducted a one-way analysis of variance. Results, as shown in Table 5 & Table 6, reveal Internet Addiction and Openness to Experiences were significantly related to computer behavior.

Table 4.5 ANOVA for Internet Addiction by Computer Behavior

Internet Addiction					
Source	*df*	*SS*	*MS*	*F*	*P*
Between groups	1	1205.419	1205.42	6.17	0.02
Within groups	93	18173.57	195.41		
Total	94	19378.99			

Table 4.6 ANOVA for Openness to Experience by Computer Behavior

Big 5 - Openness to Experiences					
Sources	*df*	*SS*	*MS*	*F*	*P*
Between groups	1	11.26	11.26	4.58	0.04
Within groups	93	228.78	2.46		
Total	94	240.04			

CHAPTER 5. DISCUSSION

The current study aimed to examine personality characteristics and traits associated with Internet addiction and their relationship to self-reported computer deviants. Using a snowball sampling method and an online survey, the current study resulted in 49 respondents who self-reported as being computer deviant compared to 46 individuals who reported never engaging in computer deviant behaviors ($n = 95$). Previous research (Rogers et al., 2006a; Rogers et al., 2006b; and Seigfried-Spellar & Traeadway, 2014) found a greater prevalence of computer deviant behavior among college samples. Specifically, Seigfried-Spellar (2014) found 60% of respondents ($n = 296$) reported engaging in a form of computer deviant behavior. The current study found the higher participants scored on the Internet addiction test the more likely they were to engaged in computer deviant behavior. However, statistical evidence revealed no correlation between time spent online and deviant computer behavior. The current study found no statistical evidence to support a difference in moral reasoning scores among computer deviants. In addition, there was no evidence to support higher manipulative and exploitive behavior scores among students classified as computer deviant or extraversion as a predictor for computer behavior.

The Rodgers, Segfried and Tidke (2006) predictive model specifically measured personality characteristics, moral decision making, and exploitive manipulative amoral

dishonesty. The current study aimed to add to the previous predictive model by also measuring Internet addiction. Personality characteristic openness to experience and Internet addiction scores were significantly correlated with computer behavior. Once entered into the predictive model, Internet addiction was the overall best predictive variable. Specifically, the predictive model successfully predicted computer deviant 51% of the time and with the predicting variables the model successfully predicted 63% of computer behavior correct.

The current study found a slight increase in computer deviance compared to computer non-deviant respondents (52% vs. 48%). Although the percentage of computer deviant to computer non-deviant is nearly split, the numbers reveal computer deviant behavior is still prevalent and continuing to occur among college students. However, the current study examined responses from both undergraduate and graduate level students, while previous research only examined undergraduate level students; this difference should be considered when reading the results.

In addition, the current study found the majority of respondents to be female ($n = 60$), with a 50/50 split between computer deviant and non-computer deviant respondents; in contrast to previous research which found 59 (87%) computer deviants to be male compared to 9 (13%) females (Rogers et al. 2006a). The current study aimed to sample the "Net-generation" which is comprised of younger generations which are more susceptible to computer and technology use. Also, statistics show that girls are receiving a high number of college degrees in recent years. Specifically, the National Center of Education Statistics (2012) found between 2000 and 2010, 60-62 percent of females received associate degrees and 57-58 percent of females received a bachelor's degree.

Regarding higher education, the percentage of master's and doctorate level degrees earned by females increased between 2000 and 2010. The increase in degree's obtained by females could also explain the increase in computer deviance among females. The findings of the current study, are different compared with previous research, and should warrant future research regarding gender of computer deviants / computer non-deviants.

Similar to Rogers, Seigfried and Tidke (2006a) the current study found no significant differences between computer criminals and manipulative /exploitive behaviors as well as no significant difference between moral decision making and self-reported computer deviant behavior. The two previous studies (Rogers et al. 2006a; Rogers et al. 2006b) offered conflicting results. For instance, Rogers et al. (2006b) found participants who were classified as computer criminals scored higher on exploitive and manipulative behavior; contrary to this, Rogers et al. (2006a) found no significant difference between computer criminals and manipulative/exploitive behaviors. Results indicate a significant correlation between computer behavior and openness to experience, specifically, you are 1 times more likely to be computer deviant if you score higher on openness to experience portion of the Big5 questionnaire. Costa and McCraw (1992) suggested that individuals who are posses the personality characteristic openness to experience are "willing to entertain novel ideas and unconventional values" and that "their lives are experientially richer" (p. 15). Previous research has not indicated openness to experiences as a significant predicting variable for computer behavior.

Although openness to experience was found significantly correlated to computer deviant behavior, Internet Addiction scores were the best predictor of self-reported computer deviance. Particularly, those who scored higher on the Internet Addiction test

were more likely to be computer deviant. Little research has begun to examine Internet addiction and computer deviance. However, McBrayer (2014) study found that script kiddie, password cracker, and old guard hacker behaviors were motivated by addiction. Although the current study found high scores on internet addiction to be significant related to Internet Addiction, there was no significant relationship between reported daily computer use and computer behavior. The author speculates the reason for the discrepancy between findings is due to the questions. Specifically, the Internet Addiction Test comprised of 20 questions with the average of the 20 responses giving a final score; while the question pertaining to daily computer use comprised of 1 question: How often do you use the computer with choices including: daily, weekly, monthly, never, I do not have access to a computer. The question pertaining to computer use does not accurately measure how often an individual utilizes the computer and for what purposes. The lack of clarity of this question could explain the difference between the significant finding of IAT and computer behavior and non-significant finding between computer use and computer behavior. Future research should continue to examine daily computer use by using more than one question.

The current study aimed to measure characteristics associated with Internet addiction and computer deviant behavior; however this is not a clinical diagnosis. Additionally, the study did not aim to determine if Internet addiction is fact or fiction, but rather determine if characteristics of Internet addiction are associated with deviant behavior. The significant correlation between Internet addiction and computer behavior could be simply because of the nature of the behaviors. It is inherent that individuals who engage in computer deviant behavior would spend more time online because there

Internet is the arena for some of their deviant behaviors. Future research should examine if Internet addiction characteristics happen *before* individuals engage in computer deviant behavior. This research could confirm or refute that Internet addiction follows a Guttman- like progression.

The current study measured hacking behaviors as a whole, while other research examined specific subsets of computer deviant behaviors. For instance, Hu et al. (2012) found moral beliefs to also play a role in hacking behaviors, specifically individuals with strong moral beliefs against hacking were less likely to engage in such behaviors. Regarding insider hacking, introversion is the most common personality characteristics among hackers (Shaw et al. 1999). The current study examined computer deviant behavior as a while previous research has looked at specific types of computer behavior.

5.1 Limitations

The current study sought a large, diverse sample size. However, the actual sample only consisted of 95 participants which attend college in nine different states. Although this is more diverse than a sample from a single university, it is still not generalizable to college students as a whole. In addition, there are some downfalls from using a non-probability sampling method, know as snowball sampling. For instance, snowball sampling can result in sampling bias and volunteer bias. The snowball sampling method allows the researcher to recruit respondents and asks them to pass the survey along to additional respondents. Sampling individuals the research knows can create sampling bias because the respondent's family and friends are likely to respond.

An additional limitation happens when using volunteer participants in research. Rosenthal & Rosnow (2009) found that individuals who volunteer in research are often

different from non-volunteer respondents. Specifically, participants who volunteer are usually more intelligence, posses a higher education level and job status (Rosenthal & Rosnow, 2009). Due to the volunteer and sampling bias associated with the current study the results gernalizibility is reduced.

 In addition, the author made an error in the use of the following surveys: EMAD, Big5 and MDKS. When uploading the surveys into the online software, Qualtrics, a single question from the EMAD, Big5 and MDKS scales were left out. The calculated Cranach's alpha for these surveys were calculated as the following: Extraversion = 0.91, Agreeableness = 0.91, Conscientiousness 0.92, Neuroticism = 0.88, Openness to Experience = 0.92, Internal = 0.88, Social = 0.55, and Hedonistic 0.73. Based on the Cronchbach's alpha reveal all of the scales had acceptable scores except for moral choice social scale. This error should be considered when interpreting the results.

5.2 <u>Future Research</u>

Previous research (Rogers et al. 2006a; Rogers et al. 2006b; and Seigfried-Spellar & Treadway, 2014) examined computer deviance among only undergraduate student, while the current study examined responses from both undergraduate and graduate level students. However, for analysis the current study did not distinguish between degree levels. Future research should look to examine difference between degree levels and/or degrees obtained by self-reported computer deviants and non-computer deviants in effort to continue to provide investigators with various characteristics to describe the individual behind the computer for cybercrimes.

Hu et al. (2012) conclude moral beliefs are a primary weapon when combating computer crime, with the current study finding mixed results compared to previous

research (Rogers et al. 2006b), future research should continue to look into exploring moral beliefs of computer deviants. Additionally, to continue to measure moral reasoning future research could look into updating the MDKS.

Subsequent research should continue to examine Internet addiction characteristics and their relationship to computer deviancy. Specifically, looking into additional characteristics researchers, such as Younger and Rodgers (1998), found to be significantly related to Internet Addiction, including: self-reliance, emotional sensitivity and rapacity, vigilance, low self-disclosure and non-conformism. In addition, researchers should look at a more accurate way to examine respondents overall computer use, as well as daily, weekly, etc. Also, research should begin to examine if Internet addiction characteristics are only significantly correlated with computer deviant behavior because of the nature of the behaviors (i.e., both take place on the computer).

Researchers have begun looking at specific subsets of computer deviant behavior, however the current study examined computer behavior as a whole. Future research should examine specific subsets of computer deviant behavior in efforts to give a more specific profile of characteristics associated with various types of deviant computer behaviors.

LIST OF REFERENCES

LIST OF REFERENCES

Anderson, K. J. (2001). Internet use among college students: An exploratory study.

Journal of American College Health, *50*(1), 21-26.

Barber, R. (2001). Hackers profiled—who are they and what are their motivations?.

Computer   Fraud & Security, *2001*(2), 14-17.

Bem, D., Feld, F., Huebner, E., & Bem, O. (2008). Computer Forensics-Past, Present and

Future. *Journal of Information Science and Technology*, *5*(3), 43-59.

Brenner, V. (1997). Psychology of computer use: XLVII. Parameters of Internet use,

abuse   and addiction: the first 90 days of the Internet Usage Survey.

Psychological reports, *80*(3), 879-882.

Caldwell, T. (2011). Ethical hackers: putting on the white hat. *Network Security*, *2011*(7),

10-13.

Carrier, B. (2002). *Open source digital forensics tools: The legal argument*. Stake.

CERN. The birth of the web. Retrieved from: http://home.web.cern.ch/topics/birth-web

Crossler, R. E., Johnston, A., Lowry, P., Hu, Q., Warkentin, M., & Baskerville,

R. (2012). Future directions for behavioral information security research.

Computers & Security, 32, 90-101.

 (2001). Digital Forensic Research Workshop (DFRWS)

Eksi, F. (2012). Examination of Narcissistic Personality Traits' Predicting Level of

    Internet Addiction and Cyber Bullying through Path Analysis. *Educational*

    Sciences: Theory and Practice, *12*(3), 1694-1706.

Elon University. 1960-1990's Internet History. Retrieved from: http://www.elon.edu/e

    web/predictions/150/1960.xhtml

Furnell, S. (2002). Cybercrime: Vandalizing the information society. Boston: Addison

    Wesley. P. 31

IC3. (2012). *Internet Crime Report 2011*. National White Collar Crime Center (NW3C).

IC3. (2012). *Internet Crime Report 2012*. National White Collar Crime Center (NW3C).

IC3. (2013). *Internet Crime Report 2013*. National White Collar Crime Center (NW3C).

IC3. (2014). *Internet Crime Report 2013*. National White Collar Crime Center (NW3C).

Goldenberg, L. R. (1992). The development of markers for the Big-Five Factor structure.

    Psychological Assessment, 4, 26-42.

Goodman, A. (1990). Addiction: definition and implications. *British journal of addiction*,

    85(11),1403-1408.

Griffiths, M. (1999). Internet addiction: fact or fiction?. *The Psychologist*.

Hinduja, S., & Patchin, J. W. (2008). Cyber bullying: An exploratory analysis of factors

    related to offending and victimization. *Deviant Behavior, 29*(2), 129-156.

Hu, Q., Zhang, C., & Xu, Z. (2012). Moral beliefs, self-control, and sports: Effective

    antidotes to the youth computer hacking epidemic. *45th Hawaii International*

    Conference on System Science, Hawaii.

Holden, C. (2001). "Behavioral' addictions: do they exist? *Science,* 294(5544), 980-982.

Holt, T. J., & Schell, B. H. (2013). *Hackers and Hacking: A Reference Handbook*. ABC-
   CLIO.

Junco, R., & Mastrodicasa, J. (2007). *Connecting to the net generation: What higher
   education professionals need to know about today's students.* Washington, DC:
   NASPA

Jones, S., Johnson‑Yale, C., Millermaier, S., & Pérez, F. S. (2009). US college students'
   Internet use: Race, gender and digital divides. *Journal of Computer‑Mediated
   Communication*, *14*(2), 244-264.

Leung, L. (2004). Net-generation attributes and seductive properties of the Internet as
   predictors of online activities and Internet addiction. *CyberPsychology &
   Behavior*,*7*(3), 333-348.

Lewis, I., Watson, B., & White, K. M. (2009). Internet versus paper-and-pencil survey
   methods in psychological experiments: Equivalence testing of participant
   responses to health-related messages. *Australian Journal of Psychology*, *61*(2),
   107-116.

Marks, J. (1990). None-chemical (behavioral) addictions. *British Journal of Addiction*, *85*,
   1389-1394.

Newburger, E. (2001). Home Comptuers and Use in the United States Retrived from:
   https://www.census.gov/prod/2001pubs/p23-207.pdf

Norton Reprot (2013). Symantec. Rretrived from: http://www.symantec.com/about/news/

Richardson, R. (2011). *15th Annual 2010 / 2011CSI computer crime and security survey*.
   Computer Security Institute.

Rogers Hospital (2014, February 24). DSM-5 now categorizes substance use disorder in a single continuum. Retrieved From: https://rogershospital.org

Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital investigation*, *3*(2), 97-102.

Rogers, M & Ogloff, JRP. (2003). A comparative analysis of Canadian computer and general criminals. *Canadian Journal of Police & Security Services*, *4,*366-376.

Rogers, M., Seigfried, K., & Tidke, K. (2006a). Self-reported computer criminal behavior: A psychological analysibs. *Digital Investigation*, *3*, 116-120.

Rogers, M., Smoak N. D., & Liu, J. (2006b) Self-reported computer criminal behavior: A big5, moral choice and manipulative exploitive behavior analysis. *Deviant Behavi or*, *27,* 1-24.

Seigfried-Spellar, K. C., & Treadway, K. N. (2014). Differentiating hackers, identity thieves,cyberbullies, and virus writers by college major and individual differences. *Deviant Behavior*, *35*(10), 782-803

Shaw, E. D., Post, J. M., & Ruby, K. G. (1999). Inside the Mind of the Insider. *Security Management*, *43*(12), 34-42.

Smith, A., Rainie, L., & Zickuhr, K. (2011). College students and technology. Retrieved from www.pewinternet.org

Selwyn, N. (2008). A safe haven for misbehaving?: An investigation of online misbehavior among university students. *Social Science Computer Review, 26*(4), 446-465.

Sussman, S., & Sussman, A. N. (2011). Considering the definition of addiction. *International journal of environmental research and public health, 8*(10), 4025 4038.

Teclaw, R., Price, M., & Osatuke, K. (2012). Demographic question placement: Effect on item response rates and means of a veterans health administration survey. *Journal of Business and Psychology, 27*(3), 281-290.

Traun, F. (1993). Addiction as a social construction: A postemprical view. *J. Psychol. 127*(5): 489-499.

Young, K.(1998). Internet Addiction: The Emergence of a New Clinical Disorder *Cyber Psychology & Behavior. 1*(3): 237-244.

Young, K. S., & Rodgers, R. C. (1998, April). Internet addiction: Personality traits associated with its development. In *69th annual meeting of the Eastern Psychological Association*.

Young, K. S. (1999). Internet addiction: symptoms, evaluation and treatment. *Innovations inclinical practice: A source book, 17*, 19-31.

Young, K. S., & de Abreu, C. N. (Eds.). (2010). *Internet addiction: A handbook and guide to evaluation and treatment*. John Wiley & Sons. .