Public Policy and Administration Research
ISSN 2224-5731(Paper) ISSN 2225-0972(Online)
Vol.8, No.1, 2018

Cyber Victimization by Hackers: A Criminological Analysis

Damian Odunze
Texas Southern University (Administration of Justice Department)
5123 Calgary Lane, Houston, Texas 77016

Abstract
The pervasiveness of the World Wide Web (internet) with the easy flow of information means that there is no more privacy once an individual goes online whether to transact business or connect with friends. Any information put online leaves an electronic trail that can be used by internet criminals, such as hackers. The recent hacking of nude pictures of more than 100 Hollywood actresses due to an iCloud leak and other cases of romance and extortion scams targeting mainly women raises a digital dilemma. This paper, using an online survey of internet users, examines whether hackers target users based on their gender. Differential association theory and routine activity perspectives are utilized to explain this new form of criminological problem. Recommendations for guarding against cyber-attacks, suggestions for future research and policy implications are also discussed.
Keywords: cybercrime, hacking, victimization, gender, routine activity, differential association

Introduction

The internet is an information superhighway, touching almost every aspect of our lives from government agencies, financial institutions, businesses, professional organizations and individuals. Although technology can deliver a number of benefits, it also introduces new vulnerabilities that can be exploited by persons with the necessary technical skills. Hacking, also known as phishing, a form of cybercrime, represents a well-known threat in online interaction and is responsible for a significant degree of disruption and damage to information systems and the internet. The recent meddling of the last presidential election in the United States by hackers supposedly linked to Russian Security agents shows the disruptive outreach of hackers. On May 12, 2017, unknown hackers launched a global Ransomware attack, nicknamed "Wannacry" or "Wanna Decryptor." Using a single malware, the hackers introduced malicious programs (worms) that infected (encrypted) over 200,000 computer systems in about 150 countries. Furthermore, there are thousands of reported cases of online individual scams, identity theft, internet fraud and attempts to dislocate the critical infrastructure of the United States and other countries. The threat by hackers increases each year as individuals, organizations, and countries rely on cyber space, information technology and computer networks to share information, conduct business and operate vital infrastructure. Cyber criminals pose serious challenges to the U.S. Department of Homeland Security and other law enforcement agencies as they battle to keep individuals and the country safe from those who seek to do harm to people through the internet.

According to the 2014 Internet Crime Report by the U.S. Federal Bureau of Investigation (FBI, 2015), Internet Crime Complaint Center (IC3) received almost 270,000 complaints related to online crime and fraud. Nearly 50 percent of the losses were financial crimes. The state of Texas, for instance, ranked third out of the states that reported complaints to the IC3 with 16,000 complaints and over $50 million in losses. The FBI noted that the complaints indicated a growing impact social media has on internet crime. The Business E-mail Compromise scam emerged as being linked to a myriad of fraud schemes. The report shows that women were victimized most when it comes to Confidence Fraud and Romance Crime (over 80%); Intimidation and Extortion Scams (over 60%), and Government Impersonation E-mail Scams (70%). Men were victimized more in auto scams (68%) and real estate fraud (63%).

This study, using a cross-sectional survey of online (internet) social network users, collected information with regard to hacking of personal e-mail and social network accounts. The researcher wanted to find out how gender relates to victimization of social network users by hackers. This current study reviewed relevant literature, and utilized a primary data: an online survey of 350 internet users, through their e-mail or Facebook accounts.

Hacking: Definition and Origin

Hacking is any technical effort used to manipulate the normal behavior of network connections and connected systems of computers. A hacker, generally, is a skilled computer user. Originally, the term denoted a skilled computer programmer, with a good knowledge of the machine and its operating system. The name arose because a good programmer is able to hack a dysfunctional system until it works. The term later assumed a negative sense to depict an individual or group who intentionally and sometimes criminally interferes with computer and network systems. Jordan (2016) gives a descriptive analysis of the geneology of hacking. As an internet crime, hacking and hackers are mainly associated with malicious programming attacks on the internet and other data networks. According to Ireland and Rush (2011), hacking involves a breach of security

mechanisms of computer and network systems without authorization, usually for the purpose of theft, destruction of information, disabling of systems, or other illegal intention. Hackers usually seek personal/financial gain or notoriety. The most common form of hacking is phishing. Hackers introduce a malware or virus to a computer/device through a malicious attachment. When a user clicks on the attachment, the virus or worm replicates itself throughout the system. Once a computer/device is affected the malware encrypts all the files and the other computers or devices in the network.

Hackers' Terminology

White Hat: This term refers to a break into computers for "genuine" reasons, often as a security specialist for corporations or government. The so called "wiretapping" by government to prevent cyber-attacks and acts of terror falls under this category.

Black Hat: This refers to a break into computer networks/systems with the intent to defraud, vandalize, or steal vital information or data.

Grey Hat: These hackers carry out similar illegal acts as the Black Hats, but they claim to do it for the public good or interest. Wikileaks and other internet-whistle blowers who hack into computer networks of government and corporations come under this group.

Hacktivist: A hacktivist uses his/her skills for political activism. Some of their acts include web site defacements, redirects, denial-of-service, information theft, and web site parodies. They use these to make statements about their political position on issues.

Government Hackers: These normally operate in collaboration with government security agencies. They can target individuals, corporations or other countries. This is a type of cyber espionage or spying used to illegally obtain information. The hacking of the DNC data and personal information of Senator Hilary Clinton by hackers allegedly linked to the Russian government falls within this category.

Script Kittie: This term refers to a novice who breaks into computer systems by using pre-packaged automated tools written by someone else. They usually have little to no understanding of what they are doing. They are the outcasts of the hacker community, and often referred to as “skidiots.” Most often, they commit these illegal acts just for fun.

Literature Review

Cybercrime is a form of white-collar crime whose growth may be as rapid and diverse as the growth of the internet itself. The term "cybercrime" may be broadly defined as any fraud or crime committed through or with the aid of computer programming or internet-related communications such as Web sites, e-mail, and chat rooms (Rush, 1999). Cyber criminals, such as hackers, use a system of social engineering to deceive their victims. "Social engineering" can be defined generally as the process by which a hacker deceives others into disclosing valuable data that will benefit the hacker in some way. Although hackers originally used social engineering to obtain codes or e-mail passwords for access to long-distance telephone lines or computers; more recent reports show that social engineering attacks can now be, and are being, used to acquire credit card numbers and other financial data (CERT, 1997; 2002-2003). Hackers and cybersecurity professionals alike recognize that social engineering involves the same techniques as criminals carrying out a traditional fraud. Some of them have also acknowledged that the success of social engineering is as a result of the application of psychological techniques for interacting with and manipulating the victim to obtain the desired information. Fraudsters exploit the natural human willingness to accept someone at his or her word. It is a hacker’s clever manipulation of the natural human tendency to trust others. It is the attempt to gain access to sensitive data (such as password, usernames and credit card numbers) by gaining human trust. Hackers break into a computer or computer network without permission. Therefore, it is certainly a criminal offense. There are individual hackers and also subgroups, such as white hat, black hat, grey hat, script kittie, hack/hacktivist, and government sponsored hackers.

Gender (victims) and Hacking

Those who hold that hackers target women more than men argue that the virtual world mirrors the natural world, where more women fall victims of crimes involving relationships, such as bullying, stalking, domestic violence and psychological abuse. In their case studies of cyber socializing and victimization of women, Debarati and Jaishankar (2009), noted that women are more vulnerable than men on social networks (SNWs). This weakness is then transferred into the virtual world of SNWs, online chat rooms, and email correspondence. The authors contend that this is the first step toward social engineering as more women are scammed into revealing their personal information. The study identified two main factors that contribute to the online victimization of women, notably, the absence of proper gender sensitive universal cyber laws and lack of awareness of the safety modes among users of the SNWs. The SNWs are considered as a large global platform to express one’s ideologies, thoughts and feelings about others. However, any individual who uses such platforms does so at his or her own risk (Wall, 2007). Unfortunately, there are less laws and policy guidelines to regulate cyber space and this lacuna inadvertently gives full freedom to the perpetrators. This is a growing phenomenon as there are now more

platforms apart from the desktop computer through which people can connect to the internet: laptops, tablets, iPads, and cellular phones. This study under review places more emphasizes on the gaps in the law and ignorance of cyber users. This current study focuses more on the perpetrators to examine whether gender is a predictive factor in online victimization.

Forms of Cybercrime

The advent of the internet of things (IOT) with a lot of devices connected to the internet, individuals, corporations and government become more vulnerable to cybercrime. Offenses targeting individuals include hacking, child pornography, cyber economic frauds, stalking (Basu and Jones, 2008); identity theft, phishing, vishing, smishing, pharming, email spoofing, morphing (Nash, 2008), cyber bombing (which is often used in relation to terrorism), cyber flame war (abusive/hate speech), cyber cheating (impersonation), cyber fraud (which is often used in relation to monetary crimes). The problem of cyber victimization is compounded by the slow response to complaints by victims. Halder (2007) did a minor research with a small sample size of 20 on the awareness of female members of Orkut, a popular social networking website. The study found that most of the respondents have never read policy guidelines before registering with the SNW, many of them checked available safety-tips only after they were victimized themselves or have heard of their friend's experiences; almost all of them have personal photographs even though they know displaying of photographs is not very safe in a public SNW. A majority of them only turned on their security button and "locked" their albums and message books only after they had experienced some sort of harassment. Some of them had their profile "cloned" and subsequently their personal information was used to dupe their friends. These cloned profiles sent friend's request to the already existing friends with the statement "I have deleted my older account, please accept me now". With this the hackers were able to gain access to the accounts of the user's friends. Some users had their profiles hacked and photographs used for pornographic purposes. These women users (whose profiles were either cloned or hacked) had deleted the old account themselves and created fresh accounts. Some had reported abuse to the Orkut authorities; some felt these incidents were not to be reported. Many of the respondents knew that posting personal photographs was not safe, yet they could not resist from showing off their photographs or those of their families or their homes to other "friends" with whom they were not very familiar. This lack of proper guardianship, as Cohen and Felson (1979) noted opens the door for hackers to come in and steal vital information.

Online Activities and Hacking

Reyns (2013) utilized binary logistic regression to study the relationships between individuals' online routine activities (e.g., banking, shopping, downloading), individual characteristics (e.g., gender, age, employment), and perceived risk of victimization on identity theft. Data from a subsample of 5,985 respondents from the 2008 to 2009 British Crime Survey were analyzed. The results suggested that individuals who use the internet for banking and/or e-mailing/instant messaging are about 50 percent more likely to be victims of identity theft than others. Similarly, online shopping and downloading behaviors increased victimization risk by about 30 percent. White and Carmody (2016) utilized focus group data to examine college students' experiences with online harassment, cyber fraud and cyberstalking. Students expressed concerns with online tracking, falsifying identities, and harassment. They also noted that incoming first-year students and those negotiating some of their first romantic relationships were especially vulnerable. Many students recommended offline programs to battle this online problem. This current study recognizes the complex nature of cyber victimization since perpetrators can disguise themselves in various ways.

It is pertinent to know that hacking often occurs in the absence of a proper "guarding" of internet networks by users. This gives the online hacker the opportunity to attack their target. This present study wanted to find out whether hackers specifically target a particular gender more than others. A theoretical framework of routine activity and Sunderland's differential opportunity theory is utilized to explain victimization of internet users by hackers.

Theoretical Framework

Philosophers and Psychologists have long debated on how human beings acquire habits and knowledge that help them to navigate the environment. Some argue that humans are born with some innate capacity to learn, while others contend that the human brain or mind is a "tabula rasa" (blank slate) and that we gain experiences (learn) as we interact with others. Aristotle (384-322 B.C) was the first to posit that all knowledge is acquired through experience and that nothing is inborn. In other words, we learn by association with others. Other philosophers such as Hobbes, Locke and Hume elaborated on this concept of "Associationism" (Bernard, Snipes & Gerould, 2010). For behavioral Psychologists, habits are acquired through stimulus and response. Cognitive theorists postulate that people learn through association with memories, ideas and expectations. Both theories go back to Aristotle's concept of association being the basis of learning.

Differential Association Theory: Edwin Sutherland (1833 -1950)

Sutherland's theory of Differential Association is the first and most dominant learning theory. The main thesis is

that criminal behavior is learned in the same way as normal behavior, through interaction with intimate persons or groups. It is not just street crimes that are learned, white collar (elite or suite) crimes, including cybercrimes, are equally learned. People (criminals as well) have mentors. Sutherland formulated his theory by drawing on three major theories from the Chicago School: ecological and cultural transmission theory, symbolic interactionism, and culture conflict theory. Sutherland (1934) underscores the point that any person can be trained to adopt and follow any pattern of behavior (either criminal or conventional) which he is able to carry out. Second, the values which the individual has cultivated are important in determining behavior. Third, certain locations (including cyber space) and people are more crime prone than others. In other words, the conflict of cultures or values is a fundamental principle in explaining crime. Differential association does not mean that mere association with criminals will cause criminal behavior. Rather, Sutherland (1939) further explained that the contents of the patterns of communication presented in association with others differ from individual to individual. The social environment and values individuals gain from significant others have an effect on their behavior. Sutherland rejected the idea that crime is the result of individual biological or mental defects. On the contrary, learning (including criminal behavior) involves acquiring ideas and beliefs in the process of associating with other people. These ideas define a person's conduct within a social context. It means that if one associates with a criminal group, the person is likely to become a criminal. Today, association is not just by physical proximity. We live in a virtual world of social, print, and electronic media: the internet, magazines/newspapers, radio and television. The portable computer and cell phone provide quick and easy access to information and association. Physical boundaries are now blurred as a result of the internet. For instance, one can learn any type of criminal behavior by going to YouTube, and connecting to any group of choice on the internet. When it comes to cybercriminals, such as hackers, there are even different cyber groups similar to the various street gangs.

Routine Activity Theory: Lawrence E. Cohen and Marcus Felson (1979)

The routine activity approach (Cohen & Felson, 1979) starts with the assumption that crime is a social reality. Crime is not attributed to any physiological or personality defects. Rather, individuals are influenced by the situation to behave one way or the other. Individuals do not make judgments in a vacuum or totally without the impact of the environment (pure determinism) or absolute free will/choice. Routine activity theory presents the social, cultural and situational factors within the environment that could have an impact on decision making. Cullen and Agnew (2003) explain further that routine activity approach deals with the factors that influence the variety of choices available to individuals. Since the environment plays an important role in decision making, routine activity does not strictly fall within the category of classic Rational Choice Theory of "absolute free-choice" (Mutchnick, Martin, & Austin, 2008). The issue of choice by the individual is secondary, similar to the soft free will of neoclassicalism (Williams & McShane, 2004). The routine activity perspective states that three components or elements must come together for crime to occur: motivated offenders coming in contact with suitable targets, in the absence of capable guardians. In the case of hackers, a suitable target could be an internet user who posts personal information online or using easily discernible passwords. This lack of guardianship creates the opportunity for the hacker to steal vital information or compromise the victim's internet account, such as online banking or email accounts. Felson (2006) further placed routine activity theory within the context of the larger human ecosystem to underscore the relationship between the offenders and victims. Crime's ecosystem, including cyber space, is constantly changing and cybercriminals keep adapting to new technologies. The internet user has to be on-guard in order not to become the next victim of hackers.

Statement of the Problem

The purpose of this study is to determine whether gender plays a significant role in the victimization of internet users by hackers (internet fraudsters). The FBI 2014 Internet Crime Report indicated almost a 50 percent variation among male and female victims depending on the type of cybercrime. It must be noted that most victims do not report their online victimization to law enforcement agencies. So, the official FBI record, at best is an underestimation. This present study raises the question: Is gender a significant (predictive) factor in the victimization of internet/social network users? This paper hypothesizes that a relationship exists between the gender of internet or social network users and victimization by online hackers. In other words, this researcher claims that having the knowledge of the gender of a social network or internet user improves our ability to predict the occurrence of victimization by a hacker. So, our level of ignorance of cybercrime/hacking (victimization) will be reduced by our understanding of the independent variable, the gender of the victim.

Methodology

For the purpose of this study, a random sample was drawn from a cross-section of internet users. Randomized "closed" questions were drawn using survey monkey (a standardized online survey website). This researcher wanted to know whether respondents have been victims of e-mail scams (hacking) or if their social network accounts have been hacked. The unit of study was individuals who have e-mails and/or use social networks (Facebook, twitter, LinkedIn, Instagram, etc.). The preliminary questions covered the age, gender, employment,

and education status of the survey participants. The remainder of the survey covered questions relating to cyber victimization (hacking). There was a pilot testing of the survey (questionnaire) with a few online users in the network circle of the researcher. After a few corrections, the survey was then sent to 380 participants in the social network circle of the researcher. Most of the participants reside in the United States. 210 of the participants were female, and 170 were males. A total of 185 females (88%) and 143 (84%) males completed the survey. All the participants were adults aged 18 years or above. The survey was focused exclusively on hacking of e-mail and/or social network accounts. For this study, frequency tables were used to describe the demographic characteristics and responses of the participants. Chi-square and phi correlation test for independence were used to measure the nominal categories of gender to determine whether gender is a predictive variable in the online victimization of e-mail and social network users and whether our level of error is reduced if we know the gender of a social network or e-mail user.

Data Analysis

The goal of this study is to determine whether gender plays a significant role in the victimization of internet users by hackers. By determining the relationship between the gender of an internet (or social network) user and victimization by a hacker, this researcher wanted to determine whether knowing an internet user's gender could help predict the prevalence of victimization by hackers.

The dependent (outcome) variable is victimization by hackers. The independent variable is the gender of the internet user. Chi test and phi coefficient (PRE) level of measurement were used to determine the relationship between the independent and dependent variables. Both variables (dependent and independent) are categorical (nominal) variables.

Table 1. Cross-sectional online survey of cyber victimization: hacking of individual e-mails and social network accounts.

	Cyber Victimization/	**Hacking of Accounts**	
Gender	E-mails hacked	Social Network Acct.	Total Accts. Hacked
Female 185	214	255	469
Male 143	135	112	247
Total 328	349	367	716

A count of internet users' e-mails and social network accounts hacked.

Figure 1. SPSS Crosstabs, Chi-square, Symmetric measures

CROSSTABS

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Gender * Cyber Victimization (Hacking)	716	100.0%	0	0.0%	716	100.0%

Gender * Cyber Victimization (Hacking) Crosstabulation

Count

		Cyber Victimization (Hacking)		
		E-mail Hacking	Social Network Account Hacking	Total
Gender	Females	214	255	469
	Males	135	112	247
Total		349	367	716

Chi-Square (SPSS)

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	5.277[a]	1	.022		
Continuity Correction[b]	4.922	1	.027		
Likelihood Ratio	5.281	1	.022		
Fisher's Exact Test				.023	.013
Linear-by-Linear Association	5.269	1	.022		
N of Valid Cases	716				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 120.40.

b. Computed only for a 2x2 table

Symmetric Measures

		Value	Approx. Sig.
Nominal by Nominal	Phi	-.086	.022
	Cramer's V	.086	.022
N of Valid Cases		716	

From the table above, the Probability of a female internet user being victimized = 469/716 = .655 or approx. .66 = 66%. The Probability of a male internet user being victimized = 247/716 = .344 or 34%. The ratio of female to male victimization by hackers is approximately 3:2.

Testing for the measures of association (relationship) between gender and the prevalence of cyber victimization/hacking of online accounts:

Ho: There is no relationship between the gender of an e-mail/social network user and victimization by hackers.

H_1: There is a relationship between the gender of an e-mail/social network user and victimization by hackers

The test statistics is χ^2 (chi-square) with df = (2-1) (2-1) = 1, at alpha = .05, the critical χ^2 = 3.841

Decision Rule: Reject Ho if computed χ^2 > critical χ^2 or if p-value (approx. sig) < alpha

Computed χ^2 5.277 is greater than critical χ^2 3.841, and p-value = .022 is less than .05, so reject Ho (accept H_1). We conclude that there is sufficient evidence that there is a relationship between the gender of an e-mail/social network user and victimization by hackers. There is a 5% chance that this conclusion might be in error.

Since there is some significant relationship, it is necessary to compute a measure of association. The appropriate measure of association is phi with a value of -.086 when squared gives us .007396 (or approx. 0.01). This means that an online user's gender accounts for about 1% of being attacked by cyber hackers. This indicates that gender is a low predictive variable in online victimization of internet or SNW users. Other factors are responsible for most incidents of cyber victimization by hackers.

Discussion

From the cross-sectional online survey of social network users who have been victimized, the results indicated a female to male ratio of 3:2, which are 66 percent female victims of hacking compared to 34 percent of male victims. Does this mean online hackers intentionally target more female than male SNW users? One has to consider other variables before reaching such conclusion. For instance, one has to think about the motivation of the fraudsters, which most often is to obtain vital information for illegal gains. Hacking and most other cyber offenses are crimes of opportunity. The gender of the victim may not be the primary consideration, but the suitability and vulnerability of the target. As the statistical analysis shows, gender is a low predictive factor when it comes to cyber victimization. Another factor is the type of online fraud being carried out. As the FBI's 2014 Internet Crime Report shows there are gender variations in cybercrime. Women are victimized more when it comes to romance and extortion scams, and more men fall victim to auto and real estate scams. However, hackers target these users because of their vulnerability. They understand the basic behavior of those who use the internet and look for loopholes to exploit. For instance, women who use online romance chat rooms could easily become victims of romance scams whereas men who gamble online could fall victim of extortion scams. Moreover, even in these cases the line gets blurred. Men have reported to have fallen victims to romance crimes, and women have been victimized in auto and real estate cybercrimes. In fact, most types of internet fraud go beyond gender lines. The recent Ransomware (Wannacry) global attack exploited vulnerabilities that existed in older versions of Microsoft Windows software. As Cohen and Felson (1979) observed, criminals attack when they notice a lack of guardianship by the potential victim. For instance, clicking on an unfamiliar email attachment could result in a malicious attack on the computer system and stealing of vital personal information by hackers. Hackers could be likened to deceptive killer animals waiting for easy prey to attack. The virtual world is akin to the real world where criminals strike "soft targets" and negligent individuals. In many instances of online victimization, the burden lies on the internet user to take plausible measures against cyber predators.

Conclusion

This study set out to examine whether the victimization of internet/social network users is related to their gender. In other words, can knowledge of the gender of an internet account holder help us to predict the occurrence of victimization by a hacker? Based on the extant literature and statistical analysis, the study established some relationship between an internet user's gender and victimization by online scammers. For certain scams, hackers tend to target a particular sex more than others, because of their vulnerability. Women, for instance, easily fall prey to romance scams, while men are more vulnerable to "big deals," such as real estate or auto scams. Although hackers target men and women relative to their vulnerability to certain types of scams, however, for most cybercrimes, particularly hacking, the line gets blurred. Other variables beyond gender come into play, including economic opportunity, age of the victim and the ease of getting information from the targeted victim. This is also in line with the findings of the FBI's 2014 Internet Crime Report. This study established that the gender of an internet user is a low predictive factor in online victimization by hackers. Cyber criminals primarily look for vulnerable targets; hence proactive-preventive measures are necessary to guard against cyber victimization.

Recommendations and Policy Implications

Prevention should be a major focus since most cyber victimization, including hacking, occurs as a result of ignorance of the risks involved in online interaction, particularly with strangers. Hacking and other cybercrimes

are criminal acts, and laws should be enacted to ensure that perpetrators are punished. This would require collaboration between policy makers (the government/security agencies) and the companies that own internet websites. The companies should put in place better security measures of detecting internet fraudsters, and also act promptly when users report abuse or attack by hackers. Consumers should also take security measures to protect themselves against cybercriminals. This includes updating the software on one's computer, laptop or mobile device to ensure that the security device is up to date. Having the latest software can be one of the best defenses against viruses, malware, and other online threats that are gateways through which hackers enter users' accounts. It is good to shred all personal information one gets in the mail before disposing them. This includes credit card applications, insurance forms, financial statements, and billing for utilities. This would prevent such crucial information from getting into the hands of criminals. Social network users should also set strict private settings to restrict access on personal network profiles to only friends, family or people the user knows. Users should set strong passwords for all their online accounts, especially online banking, social media accounts, and emails, so that they are difficult to guess. Passwords for all online accounts should be changed regularly, and should also be long, strong, and unique, with a mix of upper and lower-case letters, numbers, and symbols. By having different passwords on various accounts internet/social network users minimize the risk of multiple accounts being compromised. Furthermore, it is worthwhile to enable biometrics like fingerprint sign-in when available. Internet users should also steer clear of suspicious texts, emails and links. Unsolicited emails and pop-up ads may contain computer virus designed to steal one's usernames and passwords from his/her computer. Such emails should be deleted without opening the contents. All messages should be closed after reading or deleted. One should be careful on what one shares online. Before posting anything on the internet, including pictures and videos, users should remember that they can be used against the person. It is also good to shop at trustworthy websites. Online shoppers should look for the "s" in https:// in the URL to ensure they are shopping on a secure website. In addition, shoppers should check the seller's reputation and record of customer satisfaction on the Better Business Bureau website (www.bbb.org). Personal files stored in computers/iCloud should be backed by external hard drives/disks. Academic institutions should make "cybersecurity" a core course since a good perception of our lives is now conducted in cyber space.

Limitations

This study is limited by the use of a nonrandomized small sample. Consequently, it may not be a satisfactory representative of the population, taking into consideration demographic variables as age, income, education, and race/ethnicity. Again, the use of surveys comes with its nuance, that is, the effect of the Marshall hypothesis - people responding to questions they did not comprehend. Despite these limitations, this researcher hopes that this work has contributed positively to the body of knowledge about the victimization of internet users by hackers. Individuals who browse the internet or use social network sites should always be on guard as a careless click of the mouse or touch of the screen is a potential invitation for cyber victimization.

Future Research

There is need to study other types of cybercrime apart from hacking or internet scams, to see how they relate. For instance, one could examine how identity theft correlates with other forms of cyber-fraud. This is important because of the rise in organized cybercrime. There is also the issue of state sponsored hackers, or what Clarke and Knake (2010) call *cyber war,* that is nation-states using cyber space to covertly hack into computers and servers of other countries to obtain vital information or disrupt critical infrastructure. The recent global Ransomware attack is a tip of the iceberg to the threat cybercriminals pose to the global economy that is built on the critical infrastructure of nations. Cyberterrorism by terrorist groups and how governments are using cyber space to track potential terrorists and adversaries of the state are also potential areas of research.

References

Bernard, T. J., Snipes, J. B., & Gerould, A. L. (2010). *VOLD's Theoretical Criminology*. New York: Oxford University Press.

Basu, S., & Jones, R. (2008). Regulating cyber stalking. In F. Schmallager, M. Pittaro (eds.), *Crimes of the Internet.* Upper Saddle River, NJ: Prentice Hall.

Carnegie-Mellon Software Engineering Institute, CERT Coordination Center (1997). *Social Engineering*. Retrieved: http://www.cert.org/advisories/CA-91.04.social.engineering.htm

CERT (2002-03). *Social Engineering Attacks via IRC and Instant Messaging*. Retrieved from: http://www.cert.org/incident_notes/IN-2002-03.html.

Clarke, R. A., & Knake, R. K. (2010). *Cyber War: The next Threat to National Security and to Do About It.* New York: Harper Collins Publishers.

Cohen, L. E. & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review, 44,* 588-608.

Cullen, E. and Agnew, R. (2003). *Criminological Theory: Past to Present.* Los Angeles, CA: Roxbury Press.

Debarati, H. D., & Jaishankar, K. (2009). Cyber Socializing and Victimization of Women. *The Journal of*

Victimization, 5-26.
Federal Bureau of Investigation (2015). 2014 Internet Crime Report. *Internet Crime Complaint Center.*
Felson, M. (2006). *Crime and Nature.* Thousand Oaks, CA: Sage.
Halder D. (2007). Cybercrime against women in India. *CyberLawTimes.com, Monthly Newsletter, l 2 (6)*. Retrieved from: http://www.cyberlawtimes.com/articles/103.html.
Harl (1997). *People Hacking: The Psychology of Social Engineering.* Talk at Access All Areas III Conference. http://www.genocide2600.com/~tattooman/social- engineering/aaatalk.html
Ireland, C. E., & Rush, G. E. (2011). *The Dictionary of Criminal Justice* (7th edition). New York McGraw-Hill Companies, Inc.
Jordan, T. (2016). A genealogy of hacking. *Convergence: The International Journal of Research into New Media Technologies*, 1-17.
Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management, 11 (4),* 541-562.
Mutchnick, R. J., Martin, R., & Austin, W. T. (2008). *Criminological Thought: Pioneers Past and Present.* Upper Saddle River, NJ: Prentice Hall.
Nash, J. (2008). Making Women's Place Explicit: Pornography, Violence, and the Internet. *Module composed for open education.* Berkman Center for Internet and Society, Harvard Law School.
Reyns, B. W. (2013). Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses. *Journal of Research in Crime and Delinquency, 50 (2),* 216-238
Rush, J. J. (1999). The Social Engineering of Internet Fraud. *Internet Society Annual Conference, 1999.* Retrieved from: http://www. isoc.org/isoc/conference/inet/99/proceedings/ 3g/3g_2.htm
Smith, A. D., & Rupp, W. T. (2002). Issues in cybersecurity understanding the potential risks associated with hackers/crackers. *Information Management & Computer Security, 10(4),* 178-183.
Sutherland, E. H. (1934). *Principles of criminology* (2nd ed.). Philadelphia: Lippincott.
_____. (1939). *Principles of criminology* (3rd ed.). Philadelphia: Lippincott.
Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity: Cambridge.
White, W. E., & Carmody, D. (2016). Preventing Online Victimization: College Students' Views on Intervention and Prevention. *Journal of Interpersonal Violence.*
Williams, F. P., & McShane, M. D. (2004). *Criminological Theory*. New York: Pearson Prentice Hall.

Declaration of Conflicting Interests

The author declared no potential conflicts of interest with respect to the authorship and/or publication of this article.

Funding

The author received no financial support for the research and/or authorship of this article.