6-2018

CAN WE LEARN FROM HACKERS TO PROTECT VICTIMS?

Nicholas Marshall Chavez
California State University – San Bernardino, nchavez42100@gmail.com

CAN WE LEARN FROM HACKERS TO PROTECT VICTIMS?

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

in

Criminal Justice

by

Nicholas Marshall Chavez

June 2018

CAN WE LEARN FROM HACKERS TO PROTECT VICTIMS?

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Nicholas Marshall Chavez

June 2018

Approved by:

Gisela M. Bichler, Ph.D. , Committee Chair, Criminal Justice

Nerea Marteache, Ph.D., Committee Member

Stephen G. Tibbetts, Ph.D., Committee Member

ABSTRACT

This project examines the protection methods suggested by hackers to guard against online victimization through the lens of Situation Crime Prevention. Data were collected from 85 webpages representing three categories of electronic communications: forums, blogs, and fan pages. The goal of this project was to identify which of the 25 opportunity reduction techniques the hacking community recommend most often, as well as, what level of expertise was associated with the suggested security measures. Results indicate that the technique most recommended by the hacking community was to remove targets with 27% of the total codings. From the results three themes were found: (1) most recommendations are such that implementing the strategies would serve to protect against opportunistic, low-skilled attacks; (2) most recommendations could be considered routine precautions, that when bundled, would secure most people against cyber-theft; and finally, (3) the Situational Crime Prevention framework was not fully realized because much of cyber-theft does not involve direct victim-perpetrator interactions. From these three themes policy recommendation and limitations are presented as well as avenues for future research.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

Hacking related data breeches have dominated the news in recent times. For example, the Equifax hack is said to have leaked social security numbers and other financial data from up to 143 million people in the United States (Alfred and Musil, 2017); in 2015, the data breech of the credit reporting agency Experian affected 15 million T-Mobile customers (Weise, 2015); and, Yahoo reported that in their 2013 hack, all their user's account information, 3 billion in total, were stolen (CNN, 2017). These large-scale hacking cases have the capacity to ruin millions of lives. What is worse is that the effects of these hacks could go unnoticed for a considerable period of time and the effects can be long term, i.e., a stolen social security number could be used to take out a loan, and it could take years for a victim to reestablish their credit score following a default on this fraudulent loan. Understanding how cybercriminals, specifically hackers, defend themselves online is crucial to advancing effective protective measures against identity theft; after all, hackers are the most knowledgeable about the robustness of security measures.

This study applies the Situational Crime Prevention (SCP) framework to classify methods of protection recommended by hackers in electronic forums that are popular within the hacker community. Tallying the number of times a technique is suggested provides a rough gauge of the popularity of protective

measures. This indirectly indicates the confidence placed on the measure by the hacker community.

There is a vital need for this study because first, there is a call by researchers to look at computer crime using criminology theories (Willison & Siponen, 2009). Yet, there are few studies which examine this phenomenon through the experiences of offenders. Second, in 2016 the Internet Crime Complaint Center (ICCC) received 298,728 reports of cybercrime. The monetary losses from hacking related cybercrimes were a combined total of over 526 million dollars. Most of these victims are over the age of 60: Victims over 60 had a combined total loss of 336 million dollars. Computer crime is an extremely costly problem affecting the most vulnerable populations.

This thesis is organized as follows. Chapter 2 provides a discussion of cybercrime as well as its differences and similarities to street crime. Next, the discussion examines the main theory behind the Situational Crime Prevention (SCP) perspective, the Rational Choice Perspective, and the nine major assumptions that it makes on criminal decisions. Next, I explain SCP and how offenders use techniques to defend themselves from becoming victims. After drawing attention to the decision-making process of cybercriminals, this chapter concludes with an explanation of need to document the strategies that hackers use to protect themselves from cybercrime. Specifically, I review why the gaps in offenders as victims and cybercriminal research should be closed.

Chapter 3 describes the methods. First, I describe the three different types of web sources (forums, fan pages, and blogs) from which data were collected. From these sources, the techniques the hacker community recommended are applied to the opportunity reduction techniques of SCP. I also describe the websites used in Appendix A. Next, is a discussion of how each of the techniques were coded into NVivo; specifically, I report on how each technique was classified as a node in NVivo's qualitative coding. Finally, I conclude with the general findings of how each of the general categories were represented within the sources.

Chapter 4 contains the results of this study. First, I go over each technique and its prevalence within the hacker community. Next, I give examples of coding of each technique. Finally, in chapter 5 I go over three themes, Hacker Opportunities, Routine Precautions, and The Difficulties in Applying Situational Crime Prevention, that were found in the results. Within these themes policy recommendations are given, as well as, the limitations of this research and areas where future research could expand upon.

CHAPTER TWO

LITERATURE REVIEW

Cybercrime

Cybercrime is a destructive crime which has many ways it can be committed (Dogaru, 2012). This section seeks first, to understand the definition of cybercrime, and then, to explore its differences and similarities to street crime. Next, this section examines the different typologies of cybercrime. Following that, this paper goes on to examine hackers and why they are the focus of this research project. Finally, this chapter ends with a discussion of the harm that hackers present to society.

Definition

Cybercrime can be defined as any crime occurring on, or using a computer (Dogaru, 2001; Doyle, 2014; D'Ovidio, 2007). Cybercrime encompasses everything from attacks on infrastructure targets such as water treatment plants, internet service providers, and train networks, to trespassing on electronic resources of corporations and individuals (Holt and Bossler, 2014; Kshetri, 2009; Nasi, Oksanen, Keipi, & Rasanen, 2015). Cybercrime differs from street crime in several ways. First, given the complex and integrated nature of targets (a security breach in one internet service provider could affect millions of individual users) the scale of cybercrime, in terms of potential victims often exceeds street crime. Yet, scale is not the only difference between cybercrime and regular street crime. The biggest difference comes from the fact that people

living in separate countries can target individuals and organizations across the globe (Ibrahim, 2016; Kshetri, 2016). Furthermore, anyone with access to a computer can commit cybercrime (D'Ovidio, 2007; Holt and Bossler 2014). Moreover, the victims of cybercrime often do not realize that they have been targets of a crime (Kshetri, 2016). For example, if someone's stolen personal information was offered for sale on a cryptomarket then, unless the victim was familiar with those types of websites, they would have no idea that their private data was being bought by someone else.

On the other hand, cybercrime does share some similarities with predatory street crimes (Grabosky, 2001; Dogaru, 2012). First, some street crimes have cyber-comparatives, i.e., burglary is similar to breaking into secure sites to steal information, digital property can be taken hostage by ransomware, and phishing attacks are electronic frauds. Moreover, cybercrime motives are often the same as street crime such as earning profit or earning respect from their peers (Dupont, Cote, Savine, Decary-Hetu, 2016). Additionally, the reporting rates for cybercrime are incredibly low which can be comparable to normal crime reporting rates (Dogaru; ICCC, 2016; Kshetri, 2016); and, like street crime, cybercriminals have been known to belong to groups and organized crime syndicates (Broadhurst, Grabosky, Alazab, & Chon, 2014; LeukFeldt, Lavorgna, & Kleemans, 2017).

It is important to study cybercrime because it is disruptive and costly. The Internet Crime Complaint Center (ICCC) found that in 2016 victims' losses

reached about 1.33 billion dollars. A subset of these crimes that involved some form of hacking were estimated to be about 527 million dollars. Notably, these figures reflect crimes reported to the ICCC. Many cases go unreported due to either the victim believing that law enforcement will not take them seriously, confusion on whether their victimization is an actual crime, or because the victim is unaware that they were involved in a crime (Kshetri, 2016). This means that the 1.33-billion-dollar figure could be significantly higher.

Classification of Cybercrime

Taking a closer look at cybercrime, there are many different kinds (Dogaru 2012; D'Ovidio 2007; Doyle 2014; Holt and Bossler 2014; Leukfeldt, Kleemans, & Stol 2016). Research by Holt and Bossler (2014) expanded upon Wall's (2001) four categories of cybercrime, resulting in a general classification scheme. The first category is the *cyber-trespassing*, which is defined to include activities that constitute the crossing of invisible boundaries to access computer infrastructures that do not belong to the individual, i.e. hack into secure systems. Holt and Bossler also found that hackers are very rare. This means that a small subset of offenders engages in the prominent cybercrime cases that many see on television.

The second category is *cyber-deception and theft*. Crimes included in this category involve activities that are used to acquire another individual's information, such as their social security or credit card numbers, which are subsequently used on the internet in furtherance of other crimes, i.e., identity

theft, purchasing goods, and buying illicit products. While data acquisition activities often involve hacking, *cyber-deception and theft* does not require the use of computers. The cybercriminal can obtain personal information from hardcopy documents that are discarded in the trash, left unsecured but still in the victims' possession, through deception, or breach of trust (from documents viewed at work). Furthermore, these types of crimes do not require computer expertise. For example, when a cybercriminal pretends to be a representative calling from a bank, seeking a persons' bank account number or password.

The third category that Holt and Bossler expanded upon was *cyber-porn and obscenity.* This category involves the activity of individuals who have illegal sexual interests that use the internet to acquire videos or pictures, arrange for the production or dissemination of illicit material, or solicit illicit sex. An example of which would be websites where sex offenders can trade pedophilia videos and pictures amongst each other. Furthermore, cyber-porn and obscenity includes activities involving the solicitation of sex with children and prostitutes. Revenge porn, a phenomenon where individuals post pictures and videos of their sexual partners without their consent, is also classified as cyber-porn and obscenity.

The final category of cybercrime involves two different forms of assaultive behavior that are classed as *cyberviolence*. The first type of assaultive behavior includes activities that target individuals, i.e., cyberstalking, harassment, or threats of violence online. Research has shown that this is the highest type of crime that youths experience (Nasi, Oksanen, Keipi, & Rasanen, 2015). The

second type of assaultive behavior targets organizations and systems. For example, when hacktivists break into a computer system not to steal information, but to cause harm or to humiliate an organization they do not agree with, their actions could be classified as assaultive behavior.

The focus of the present study is on preventing *cyber-theft*. This is accomplished by examining the security advice given by members of hacking communities who could be involved in cyber-trespassing and/or using cyber deception to break into websites or computers to either steal information or to show off. The scope of this paper does not include coders who are individuals that create tools for hackers, i.e., Malware programs which activate on an individual's computer without their knowledge and steals information (Dogaru, 2012). Hacker tool creation is excluded from the study because these people do not actively seek to commit cyber-theft they only create the tools.

Hacking and cyber-theft are important to focus for several reasons. First, the ICCC reported that there was a total of 43,094 instances which involved hacking. Second, there is a need for computer crime to be researched using criminology theories (Willison & Siponen, 2009). Third, 64 percent of hacking instances examined by the ICCC involved cybertheft of personal data. Typically, someone had their own computer either hacked or compromised and their personal information stolen.

Hackers

The age of the typical cybercriminal ranges from 20-35. Most offenders are predominantly male, and they are familiar with the system that they are trying to break into or know people who are familiar with the systems (Dogaru, 2012). Most hackers do not have a criminal history and have a good social status. Individual motivations vary, but most people report that they are either motivated by money or by their status (Dogaru, Holt and Bossler, 2014; Seebruck, 2015). Finally, hackers can either work by themselves or in a group, however when hackers do work in a group they are rarely organized (Choo, 2008; LeukFeldt, Lavorgna, Kleemans, 2017).

Classifying hackers and hacking groups by both their skill level and motivational factors, Seebruck (2015) created an updated typology model that separated hacker motivation into five distinct categories: prestige, ideology, profit, revenge, and finally recreation. To ensure flexibility, Seebruck's typology also allows for hacking groups and hackers to have multiple motivations for their cybercrimes. This follows previous research which has suggested that cybercrime groups typically do not have a strict leadership therefore individuals in the group might initiate activity for different reasons (Broadhurst et. al., 2014).

Prestige hackers are those who hack to gain respect in a forum, website, or other form of community. By reporting their exploits and the methods these hackers hope to earn the trust of their peers, thus improving their position (Dupont, Cote, Savine, & Decary-Hetu, 2016). This category can also include

coders, people who develop the ways that hackers can break into systems (Dogaru, 2012). Coders can also gain respect by providing tools for hackers in other categories.

The next category in Seebruck's (2015) typology are *ideological hackers*. These individuals include those who refer to themselves as hacktivists. What this means is that these individuals are aligned with a larger cause. Instead of using their knowledge to earn trust or monetary gain, they use their skills for a so-called greater good (Seebruck, 2015). The people in this category include groups like Wikileaks who believe that information should be free to everyone. This category can also include state actors such as those who created the Stuxnet virus to attack the Iranian nuclear program.

The third category are those who are motivated by *profit*. The main concern to this group is how to earn the greatest amount of money from individuals or from businesses. These hackers primarily target personal information that can be sold online, such as credit card and social security numbers. Furthermore, they could use this information to make fraudulent charges or take out loans in the individuals' name.

The fourth type of hackers are those who are out for *revenge*. This group believes that they have been wronged in some way and want to "get back" at those who have wronged them. The prime example of this type of hacker is the group Anonymous. For example, this group took down the Prime Ministers' website after he sought to censor offensive content on the internet (Zetter, 2009).

The final type of hackers are recreational hackers. This group participates in hacking because they feel a need to challenge themselves or they want to expand their skillset. Recreational hackers also post about their exploits to gain attention. These are also the groups who attend hacking conventions to figure new techniques and make connections within the community. While these groups might want to know hacking for fun, there are also those who hack to prove their abilities to their peers.

Harm

In total the ICC received 298,728 reports of cybercrime in the year 2016. The group with the most victims were those who were over the age of 60 with around 18.4% of victims. The next closest age group were those between the ages of 30-39 with around 18.3% of victims. As for monetary losses, those over 60 suffered the most with an estimated loss of around 339,474,918 dollars.

Cybercriminals are just as susceptible to crime as non-criminals. This is because even though some people have more technical skill and knowledge about security, as a group, individuals are likely to spend a lot of time online, and more exposure suggests a greater potential for victimization (Pratt, Holtfreter, & Reisig, 2010). Since cybercriminals have more knowledge of the effectiveness of security measures, their knowledge and experience with cyber-theft provides great insight into internet enabled crime. Moreover, cybercriminals use the same technology as non-cybercriminals. Therefore, their computers would contain the same vulnerabilities that allow them to be hacked.

After examining what cybercrime is and how it affects those who are victims of it, one can see why figuring out which SCP techniques are effective against it is important. It is also crucial to understand Rational Choice Theory before applying SCP. This is because Rational Choice theory is one of the main theories behind the SCP perspective.

Theoretical Framework

Rational Choice

The Rational Choice perspective is derived from two concepts: utilitarianism, and traditional economic choice theory (Adler, Mueller, & Laufer, 2010). What these two theories state is first; all choices people make are to maximize pleasure and minimize pain. Second, is that people will weigh their options and choose whichever option will satisfy their needs the most. Rational Choice combines these two idea to theorize that criminals will make the decisions from those two theories intelligently and with free will. This means that when someone goes out and commits a crime they do so because they conclude that the possible benefit of that crime outweighs the possible costs of getting caught. Furthermore, when they make that decision, they are not influenced by any other factors besides their own decision-making process (Adler, Mueller, & Laufer, 2010).

McCarthy (2002) theorized that there are nine general assumptions that Rational Choice makes about offenders. (1) People have desired outcomes that they would like to achieve. (2) Those outcomes are complete, transitive, and

stable, meaning that they have a least desirable outcome and most desirable outcome. Furthermore, there is a consistency to the outcomes that are desired. (3) Present and future benefits influence people's preferences. This means that to take a future option that benefit must be greater than the present offer. (4) Outcomes are not set in stone, in other words, uncertainty influences a person's preferences. (5) People use the information that they accumulated to base their assessments on costs and benefits. (6) Rational actions are based on the above assumptions. (7) Is the assumption that rational choice perspective does not assume everyone will make the most rational decisions and that emotional states influence choices. (8) People's choices fall into either a decision or game theory approach. Decision theory means that only that one person's decision and chance affect the outcome. Game theory states that more than one persons' decision influences the outcome. Finally, (9) is the assumption that rational choice is not a theory of cognation. This means that it does not posit that there is a right way to think, only that people's choices are consistent.

Another important aspect to look at is how offenders choose their targets. Research looking at burglaries, the closest approximation to cyber-trespassing, found that many different factors are at play when a burglar chooses their targets (Townsley, Birks, Ruiter, Bernasco, & White, 2015). Preferences, morality, and ease of access have all been found to be related to target selection (Breetzke and Cohn, 2013; Taylor, 2014; Townsley et. al., 2015). Research on drug dealers

also showed that those who looked easy to rip off were targeted (Jacques, Allen, & Wright, 2014).

There are two important ideas that can be taken away after examining Rational Choice Theory. First, is that criminals make choices that are rational. Second, is that these choices are based on the factors surrounding the crime they want to commit. What these two ideas mean is that there is a clear way to dissuade criminals from committing crimes. This means that there is a clear way to dissuade criminals from committing crimes. To accomplish this, according to Rational Choice, one must make the cost of committing a crime outweigh the benefits.

The next perspective looked at, SCP, aims to increase the disadvantages of committing a crime. It is reasoned that increasing disadvantages over anticipated rewards would lead potential offenders to refrain from committing a specific crime. Disrupting rational decision-making process will prevent crimes. Since hacking is often a pre-cursor crime to cyber-theft, it follows that if cybercriminals were dissuaded from hacking, the cybertheft should decrease as well.

Situational Crime Prevention

Situational Crime Prevention is a perspective that builds off many theories such as Rational Choice Theory, Routine Activities, and Deterrence theories of crime. To fully understand this perspective this section first outlines what SCP is and the perspectives' main aspects. Next, this section examines how offenders

could use SCP to defend against threats. Finally, this section looks at how this relates to cybercriminals and their decision-making process, as well as, why one should examine their use of SCP.

The main objective of Situational Crime Prevention is to remove the opportunities for crime (Clarke, 2010). To facilitate a comprehensive approach to opportunity reduction, Clarke proposes a framework comprised of 25 techniques that aim to persuade a potential criminal offender that the cost of committing a crime outweighs the benefit of that crime, whilst removing excuses for criminal activity. Clarke (2010) also posits that the opportunity-reducing measures have three components. The first is that they are directed at a specific form of crime. The second is that it involves some sort of change in an environment that is as permanent as possible. Finally, these changes make crime riskier to the offender or provide the offender with less reward. SCP does not seek to explain the crime, but to prevent the crime from taking place (Clarke, 2010).

Clarke (2010) proposes that there are five aspects that if modified, can prevent crime, by influencing the offender's assessment of crime opportunity—increasing the effort required to commit the crime, increasing the risks of detection and apprehension, reducing the rewards that may accrue from the crime, removing the provocations that may trigger offending behavior, and finally, removing the excuses that may be used by offenders to justify their actions. Within each category, Clarke (2010) proposes specific opportunity reducing techniques, resulting in a total of 25 opportunity reducing techniques that can be

applied to dissuade criminals from choosing and acting against targets. In the text that follows, I explain the SCP framework in greater depth.

The first category proposed by SCP is to *increase the effort* it takes for a criminal to commit a crime. Within this category are five techniques: target hardening, control access to facilities, screen exits, deflect offenders, and control tools. Target hardening involves making the victim harder for potential criminals to access. Examples of which include: steering wheel locks, deadbolts for doors and bars covering windows. The next technique is to control access to facilities. For example, having a pass code to gain access to potential burglary targets. Screening exits involves placing mechanisms or personnel in such a position that there is continual surveillance of egress, i.e., having a security guard at the exit door or attaching merchandise tags that emit a sound when leaving through a door. The fourth technique is to deflect offenders. This involves making it difficult for an offender to commit the crime. An example of this would involve having separate seats for fans of opposing teams at a sporting event. Finally, Clarke (2010) argues that increasing the effort to commit a crime could be accomplished by controlling the tools used to commit the crime. This would mean restricting the sale of certain products like medicine or bolting down chairs in bars.

The next category is *increasing the risk* of detection and apprehension. For this category the first technique is to extend guardianship. For example, when leaving for the night one would keep a light on to give the illusion that somebody was home. Next, is assist natural surveillance, this would entail cutting

down branches in a heavily shadowed area. The third technique is to reduce anonymity, for instance using real names as users on a computer. Next, is to use place managers, these would include security cameras or more cashiers in a gas station. Finally, is to strengthen formal surveillance. What this means is to have systems in place like burglar alarms.

The next category is to *reduce the rewards* offenders may gain from criminal activity. The first technique is to conceal the target, for instance keeping high valued electronics behind the counter of an electronics store. The next technique is to remove the targets. An example of this would be steering wheels that are detachable and are brought with the driver. Next is to identify property, i.e. vehicle identification numbers, thus, making it harder to sell on the black market. The fourth technique is to disrupt those markets. For example, cracking down on websites that sell private information. Finally, is to deny the benefits, for example, safes that permanently lock after too many wrong passwords.

Next, is to *reduce provocations* that induce crime. The techniques in this category include reducing frustration and stress such as creating an orderly venue during sporting events. After that, is to avoid disputes between people. Next, is to reduce the temptation and arousal such as banning prostitution. Fourth, is to neutralize peer pressure. Finally, is to discourage imitation such as fixing broken windows.

The last category is to *remove excuses* for crimes. The techniques used in this category are first to set rules. This could mean anything from lease

agreements to no loitering signs. The next technique is to post instructions. For example, signs specifying where to park. After that, is to alert their conscience. This includes posting signs about the harm of shoplifting. The next technique is to assist compliance. This means to have facilities for homeless people and regular people to use the restroom. Finally, is to control drugs and alcohol. An example of this would be the breathalyzer in a car needed to start.

There have been numerous studies that have investigated the utility of the SCP framework and the effectiveness of specific techniques in reducing crime (Clarke, 2010). For example, research on steering wheel locks has shown significant reductions in motor vehicle thefts (Webb, 1994). SCP has also been shown to reduce prostitution, obscene phone calls, burglary, car crime, as well as return fraud (Anderson & Pease, 1994; Challinger, 1996; Clarke, 1990; Matthews,1990). Andresen and Felson (2010) also showed that SCP can be used in unison with other theories to develop effective and comprehensive crime reduction initiative. Researchers in this study combined SCP with co-offender theories to broaden SCP's scope to include social crimes. (Andresen and Felson, 2010).

Furthermore, SCP has been used to develop strategies to defend computer systems. Willison and Siponen (2009) came up with a modified version of Clarke's SCP that applied each of the 25 techniques to computer systems. Research by Hinduja and Kooi (2013) also found that applying SCP would benefit the information security sector.

In the research study by Willison and Siponen (2009) they used crime scripts to tie insider computer crime with SCP. They showed that practitioners could use crime scripts to come up with effective SCP opportunity reduction techniques that would benefit their specific needs. Furthermore, the researchers showed that SCP could be applied to cybercrime by providing some examples of opportunity reduction techniques that focused on computer crime. In the conclusion of their paper Willison and Siponen called for computer crime to be examined through criminology theories.

Finally, Hinduja and Kooi (2013) posit that SCP can be applied to information security (InfoSec). They go on to state that not all aspects of SCP can be applied and that there are only 16 of the 25 techniques that can be applied. These researchers also state that there are two main limitations to how SCP can be applied to InfoSec. The first is that there is cause for concern for adding more surveillance to the online ecosystem. Second, they state that it takes time for security measures to be implemented making it difficult to implement when the InfoSec world changes rapidly.

Offenders' use of Situation Crime Prevention

Offenders are often overlooked when it comes to research about victims. However, offenders routinely employ techniques to protect themselves from law enforcement, other criminals, or from upset customers (Jacques, Allen, & Wright, 2014; Jacques and Reynald, 2012; Piza and Sytsma 2016). Some techniques

that offenders use vary by the time of day that their activities take place in (Piza and Sytsma, 2016).

Looking closely at the research: Piza and Sytsma (2016); Dickinson and Wright (2015); Jacques, Allen, and Wright (2014); and Jacques and Reynald (2012) all looked at offenders as victims. Piza and Sytsma (2016) and Dickinson and Wright (2015) both examined how drug dealers defend themselves from law enforcement. Piza and Sytsma's (2016) research involved the defensive techniques of open-air drug dealers, those who sell on the street, in New Jersey. Using the Newark Police Departments security cameras, researchers were able to identify that drug dealers preferred to operate out of view of place managers, people who regularly interact with the street. Furthermore, they found that drug dealers used situational prevention techniques in the spots where they stashed their drugs. Dickinson and Wright (2015) also examined how drug dealers use gossip to protect themselves from being arrested. Using data from interviews with drug dealers' researchers found that they used that information to make informed choices as to when to stop selling, who to avoid, and what strategies they use to avoid these threats.

Jacques, Allen, and Wright (2014) looked at drug buyers and the choices that drug dealers make when they defraud them. Using interviews with drug dealers the researchers found that those who are unlikely to retaliate or are unable to take their business somewhere else are most likely to be ripped-off. Jacques and Reynald (2012) looked at drug dealers as victims. Seeking to

examine whether offenders use situational prevention techniques to defend themselves from victimization, the researchers conducted interviews with 50 drug dealers. What they found was that offenders employed all five main categories of SCP, increasing the effort; increase the risks; reduce the rewards; reduce provocation; and remove excuses, in some form to protect themselves.

While normal citizens must worry about criminals taking advantage of them or harming them and businesses must worry about upset customers, offenders often must worry about both as well as law enforcement (Jacques and Reynald, 2012). There are also drug buyers who are typically victims of crimes (Jacques, Allen, & Wright, 2014).

As Jacques and Reynald (2012) pointed out, there is a need to understand offenders' use of techniques to defend themselves because there are some techniques that are unknown to most people. Most people would not know the intricacies of the criminal world and what methods are truly effective in protecting oneself from crime. Understanding the criminals' perspective allows individuals to gleam the most effective ways to protect themselves. This is because these are the people who commit the crimes, therefore, the methods they employ will be the most effective measures to stop those types of crimes.

These techniques, while not tailored to the cybersecurity field, have been used by Willson and Sipinen (2009) in a cybersecurity orientation. There are two main limitations to this study that the current study seeks to resolve. First, is that this study looks at preventing crime from an InfoSec perspective. The techniques

recommended are geared towards practitioners in the corporate world. Second, the study only focuses on one case of criminal behavior and does not have a sample.

Table 1. Situational Crime Prevention Table Applied to Cybersecurity

Increase the effort	Increase the risks	Reduce the Rewards	Reduce Provocation	Remove excuses
1. Target Hardening: • Anti-virus software • Installing a Firewall	6. Extend guardianship • Monitor PC functions	11. Conceal Targets • Hide Wi-Fi network • Conceal PC name on public networks	16. Reduce Frustrations and stress: Host hacking challenges with prizes	21. Set rules • More disclaimers on forums about only hacking computers that an individual owns
2. Control Access to facilities • Password on crucial computer functions • No one else uses computer	7. Assist natural surveillance • Improved street lighting	12. Remove targets • No personal data on PC • Computer resets to previous configuration	17. Avoid disputes • Do not post inflammatory statements	22. Post instructions • "No Parking signs"
3. Screen Exits • Export Documents • Reception desks	8. Reduce anonymity • Link forum users to a verified Facebook account	13. Identify property • Monitor dark web for personnel identifiers	18. Reduce emotional arousal • Do not promote hacking videos or posts	23. Alert conscience • Have pictures of family on PC
4. Deflect Offenders: • Disconnect important computers from the internet	9. Utilize place managers • Automatic Firewall monitoring • Check on PC for weird behavior	14. Disrupt Markets • Take down dark web markets	19. Neutralize peer pressure • Do not encourage people to attempt to hack	24. Assist compliance • Set up fake websites for other hackers to try their skills on
5. Control tools/weapons • Monitor who has access to botnets	10. Strengthen formal surveillance • Intrusion Detections system	15. Deny Benefits • Encryption on data files in computer	20. Discourage imitation: • Update computer software after the fact.	25. Control drugs and alcohol: • Do not use the computer when drunk

Source: Willson and Sipinen (2009)

Current Study

The reason cybercrime should be investigated is because cybercriminals are just as much victims to online attacks as regular citizens. Research has shown that the more time spent online means the likelihood of being a target of internet crime is increased (Pratt, Holtfreter, & Reisig, 2010). Therefore, knowing how hackers defend themselves gives more insight into how average citizens can defend themselves. This ties into what Jacques and Reynald (2012) said about regular criminals. There is a need to know the strategies criminals employ to better protect ourselves.

The reason there is a need to understand criminal techniques is because they are experts in their field. Therefore, if they want to protect themselves from the crime that they commit, then they should know what will stop other criminals in that same category. This is particularly true for hackers' knowledge because most computers operate in the same way. Thus, the techniques that they recommend for their own sub-group will work on non-criminal's computers just as effectively. There is also a need to look at whether this advice could be used by computer novices or those with expert levels of computer knowledge.

Examining the body of research, there are few studies that examine what cybercriminals protect themselves from. It can be inferred that the same criminal risks that exist for regular people exist for cybercriminals because of the amount of time that they spend on the computer (Pratt, Holtfreter, & Reisig, 2010).

Malware and Phishing attempts do not discriminate when it comes from sources that are anonymous. Furthermore, one can assume that to gain respect, a hacker might try to break into another fellow hacker's computer. Thus, the same kind of decision making process might occur in cybercriminals minds as those of regular individuals.

As stated above, there is a limited amount of research on offenders as victims. Furthermore, even if high-profile hacks are a popular subject in the news, there is little research on techniques to defend oneself from hacking. This current study seeks to close both gaps by examining the protection techniques used by those in the hacking community.

The primary goal of this exploratory study is to document the techniques that hackers use to defend themselves online. Specifically,

Q1. Do the protection techniques of hackers fit within the framework of SCP?

Furthermore, if they do use SCP techniques, then which categories are most likely to be recommended? The reason one should look at these techniques is because if the individuals who are entrenched in the hacking community are using these methods, then those methods would be effective for the online habits of everyone. Second,

Q2. What level of expertise is needed to follow the advice recommended by the hacker community?

The reason this question is important is to determine whether these techniques can be used to protect average citizens from becoming victims of cybercrime.

CHAPTER THREE

METHODS

Data Source

Data were collected by performing a content analysis of 24 websites that have some connection to the hacking community (see Appendix 1 for list). Qualifying websites included having some connection to the hacking world, for example sites that are dedicated to hacking news or strategies. Furthermore, these sites must not be selling some security software or service. The sites that met these criteria were found using a basic google search using the terms “hacking”, “hacking community”, “hacking forums”, and “hacking sites” as well as through websites that linked other hacking related websites. The reason for this terminology is that these terms are the best descriptors available for those who hack. Examining these sites, three main categories were observed: forums, fan pages, and static posts/blogs. It is important to note that the only Fan Page website that was included within this analysis was the website Reddit. From these sources, units of measurement were collected from each webpage.[1]

1. Forums are websites that contain message boards for a subject (see Figure 1). Inside of these message boards users make posts that other users can then respond with their own posts. Forums must be created by individuals who

[1] Originally this project sought to capture videos, however there was not enough video sites with accessible data to search through. Furthermore, this project wanted to capture exposure rate of each technique recommended. Still, like videos there was not enough data to capture this metric.

understand how to code webpages and must pay for a server to host their website and forums typically only cover one subject area. Users of these forums can take on multiple roles. For example, there are administrators who run the website, moderators (mods) who control what people can post on these forums, as well as, control which parts of the forums other members can access. Finally, there are users who can only post and read what the moderators allow them. Some forums have systems in place where an individual must register for the community before they can view or interact with posts. In total two major forums were found in the initial search. The posts inside of the forum were the unit of measurement collected. Furthermore, any replies by users were included in the analysis.

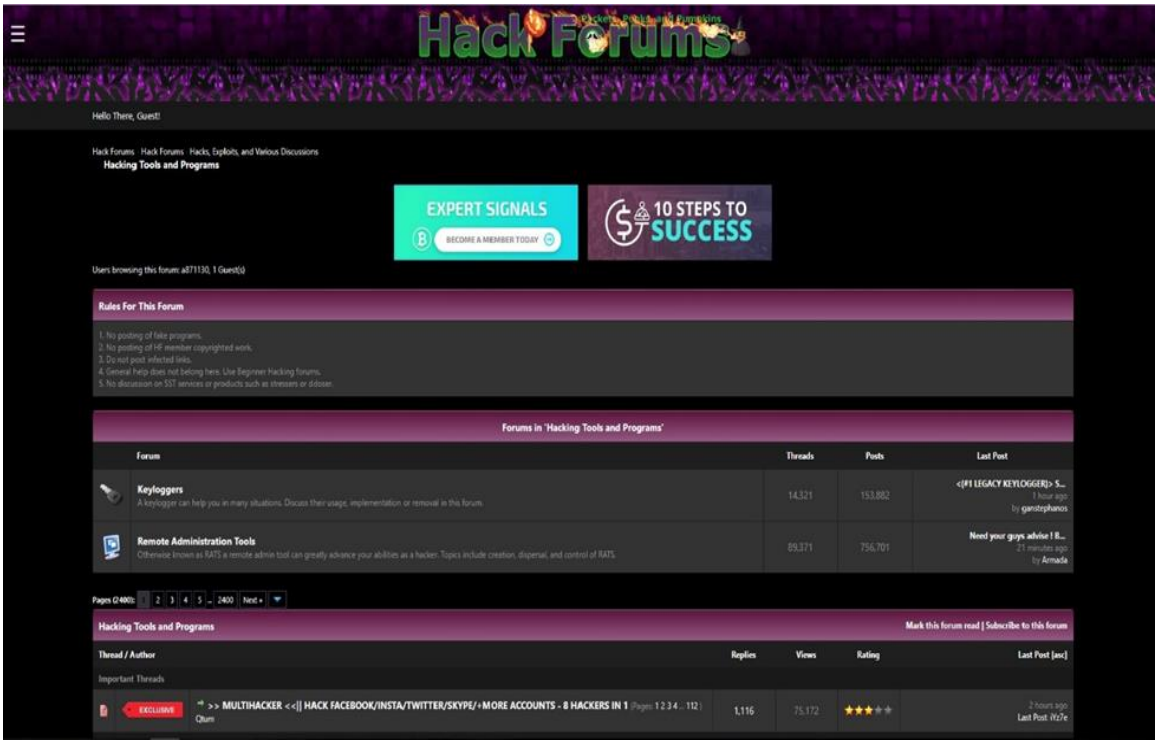

Figure 1. Forums (hackforums.net)

2. Fan pages are categorized, like forums, as places where users can post topics of conversations for others to post replies. Fan pages can be created by any individual. These pages are then hosted on a larger website alongside other fan pages of varied interests. For instance, there can be one fan page created about dogs and another fan page about hacking all on the same website. Fan page websites have their own administrators and moderators that can control any fan page. Individual fan pages can then have their own set of administrators and moderators. Finally, users of these larger sites can visit these fan pages and post onto them once they become members of that community. There are some fan pages that make entry into their community restricted. What this means is if an individual wants to read the fan page one of those fan page's that are

restricted, then an admin would have to approve them. Four fan pages were included in this initial search from the larger fan page site Reddit. Like forums, posts and user interactions were collected as the unit of measurement.

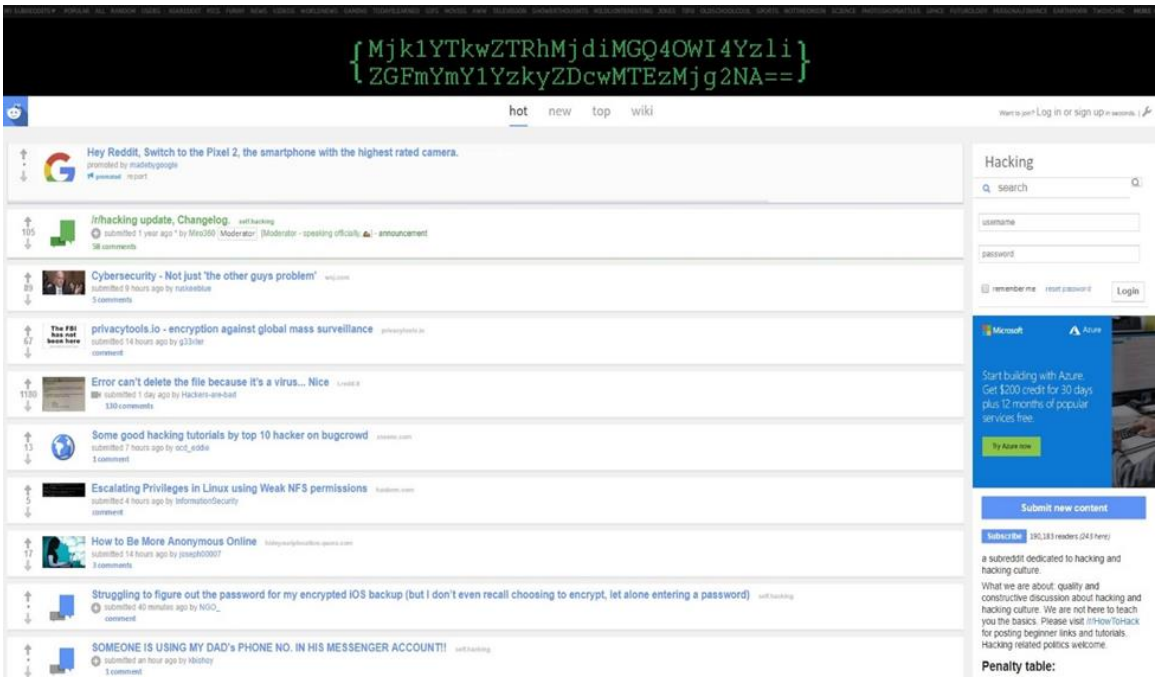

Figure 2. Fan Page (reddit.com/r/hacking/)

3. Static posts/blogs were the most prevalent data source. Static posts are blogs or websites (see Figure 3) that display articles that are written by people knowledgeable in the hacking field or participate in hacking activities. These websites contain information either to teach or to inform users. Interaction amongst users within these types of websites is limited. For instance, some websites do not have comment sections. Data were pulled directly from the

article. Also, if there is a comment section, data were pulled from those interactions. In total, there were 18 blogs included in this study.

Figure 3. Static/Blog (thehackerblog.com)

Sample

For blogs and forums, a search was performed looking for posts that contain tips and strategies for protecting oneself online. For fan pages first, a search was performed within the site using the terms “hacking”, “hacking community”, and “hackers”. This allowed the finding of hacking communities on these sites. Next, like with blog posts, a search was conducted on strategies that one can use to protect themselves online.

Data collection lasted from 12/21/2017 to 01/16/2018. In total, 134 websites were identified, and from those websites, 24 contained useable information. Two of these 24 sites were forums, four were fan pages, and finally, 18 were static posts/blogs (75% of sites examined were static posts or blogs). The pages used in this study were found by using the search terms “security”, “protection”, “safety”, “protect”, “protect yourself”, “protection tips” and “safety tips” within the various sites. It was found that 85 web pages had information useful for this study. Within those pages, I found 379 references to specific protection techniques; notably, some techniques were mentioned several times.

Data Analysis

Data were processed through the qualitative data analysis software NVivo. NVivo was chosen as the software to analyze this data because of its functionality and previous use in a cybercrime study (Hutchison, Johnston, & Breckon, 2010). For example, NVivo allows for a quantitative analysis on qualitative data (Bazeley, 2002). This means that even with a large amount of qualitative data, analysis can be done in a shorter and more efficient time. Moreover, research by Barratt, Lenton, Maddox, and Allen (2016) used the software to analyze interviews with cryptomarket users.

Each strategy named in a webpage as a technique that could be deployed by an individual to being victimized was captured as a node. To code blog posts, first each relevant article page was downloaded through the NVivo capture tool on the Chrome browser. Next, the page was examined for techniques

recommended. Coding forums worked like fan pages. First, all posts that showed up either asking for tips or offering tips on protection, were downloaded through the same software as blog articles and stored within the NVivo software. Next, the entire post along with user comments were examined and any mention of protection techniques were coded into the appropriate node.

In addition, each technique was rated as either expert, meaning the advice was intended for users with extensive computer knowledge, or novice, which was advice where little to no computer knowledge was needed. A piece of advice was considered expert if that advice recommended strategies that involved a user either changing computer coding or other actions that could not be set in a program's settings. An advice was coded as novice if a user could accomplish that advice with little to no effort or simple setting changes.

Once found, the technique was highlighted and coded into a node on the NVivo software. Each node was labeled with one of the 25 opportunity reducing techniques of SCP (see Table 2). For example, if a blog article recommends a specific anti-virus, then that part of the article was coded into the node labeled Target Hardening. Or, if someone asks a question on which firewall to use on their computer and a user responds with a certain firewall, then that answer was coded into the Target Hardening node. The full list of 25 opportunity reducing techniques of SCP was on hand to ensure reliable coding. Examples for each technique were drawn from a prior study of cyber SCP by Willson and Sipinen (2009). However, if a technique was not represented within the five categories,

then that technique was placed under the best fitting technique. Furthermore, if a strategy closely matched other techniques then only one was chosen.

In addition to a generating an updated catalogue of prevention strategies, this study aimed to reveal how advanced each technique being advocated. First, a tally of each technique advocated from the data pulled by NVivo revealed which techniques the hacking community value the most. These were then matched with one of the 25 opportunity reducing techniques as closely as possible, an example of which can be seen in Table 2. After everything was matched the techniques advocated the most are shown in the table.

Table 2. Situational Crime Prevention Table

Increase the effort	Increase the risks	Reduce the Rewards	Reduce Provocation	Remove excuses
1. Target Hardening	6. Extend guardianship	11. Conceal Targets	16. Reduce Frustrations and stress	21. Set rules
2. Control Access to facilities	7. Assist natural surveillance	12. Remove targets	17. Avoid disputes	22. Post instructions
3. Screen Exits	8. Reduce anonymity	13. Identify property	18. Reduce emotional arousal	23. Alert conscience
4. Deflect Offenders	9. Utilize place managers	14. Disrupt Markets	19. Neutralize peer pressure	24. Assist compliance
5. Control tools/weapons	10. Strengthen formal surveillance	15. Deny Benefits	20. Discourage imitation	25. Control drugs and alcohol

During data collection it was found that no category was present in every source, as seen in Table 3. Across 85 separate pages, 68%[2] contained some form of Increase the Effort and 67% of pages contained techniques related to Reducing the Rewards. Increasing the Risks were only present in 36% of pages and 31% of pages contained Reduce Provocation techniques. Finally, no page had techniques that related to remove excuses. In terms of skill sets, 77 pages advocated prevention strategies that could be used by novice computer users. On the other hand, only 21 pages contained advice intended for those with expert levels of computer knowledge. Some of these pages contained both expert and novice advice.

[2] Percentages do not add up to 100% because one source could contain multiple techniques. For example, one page could have Increase the Effort as well as Reduce Provocation.

Table 3. Sample Description, n=85 pages

Variable	Frequency	Percent
Sources		
Forums	20	24%
Fan Pages	17	20%
Static Posts/Blogs	48	56%
Technique Category		
Increase the effort	58	68%
Increase the risks	31	36%
Reduce the Rewards	57	67%
Reduce Provocation	26	31%
Remove excuses	0	0%

CHAPTER FOUR

RESULTS

This results chapter is organized as follows. First, a table is shown detailing the different techniques of SCP and their representation within the data. Next, this section shows examples the most recommended strategies by the hacking community. This is then supplemented with quotes that were used to create these samples. Finally, this section answers the second research question posed about whether the techniques recommended could be used by those with limited computer knowledge.

Prevalence of Opportunity Reducing Techniques

The primary impetus to this study was to determine whether the cybercrime protection techniques discussed within the hacker community fit within the framework of SCP. If the SCP framework was feasible, then the inquiry turned to investigating which class of techniques were most prevalent. Table 3 reports how the sample of 379 advisements, found within 85 unique webpages, fits within the SCP framework. Of note, there were no instances of suggestions that fit any of the categories within the removing excuses technique. The two most prevalent categories were increase the effort and reduce the rewards, 34% and 46% respectively. Table 4 reports how common opportunity reducing technique were relative to each other (N=379 coding's).

Table 4. Results

Increase the Effort	**Increase the Risks**	**Reduce the Rewards**	**Reduce Provocation**
34% (128)	**11% (41)**	**46% (174)**	**9% (36)**
Target Hardening **12% (45)**	Extend Guardianship **2% (9)**	Conceal Targets **18% (69)**	Reduce Frustrations & Stress **0(0)**
Control Access to Facilities **8% (30)**	Assist Natural Surveillance **.7 % (3)**	Remove targets **27% (101)**	Avoid Disputes **.5% (2)**
Screen Exits **.2% (1)**	Reduce anonymity **0**	Identify property **0**	Reduce emotional arousal **1% (4)**
Deflect Offenders: **13% (48)**	Utilize place managers **4% (17)**	Disrupt Markets **0**	Neutralize peer pressure **0**
Control tools/weapons **1 % (4)**	Strengthen formal surveillance **3% (12)**	Deny Benefits **1% (4)**	Discourage imitation: **8% (30)**

Note: Percentages are based on grand total

Increase Effort

Within this category the most common technique mentioned was deflecting offenders (13% of coding). Advice given included the following:

- "Use Pegasus or Thunderbird (by Mozilla), or a web-based program such as Hotmail or Yahoo (In Firefox)."
- "Use Strong passwords"

- “While you download files from untrusted websites/sources such as torrents, warez etc. make sure that you run a virus scan before executing them.”

Exploring the frequency with which each strategy was mentioned, using a strong password showed up the most frequently with 9 instances. Next, were recommendations to use safer software such as Firefox or Linux (6 instances) and to change passwords often (6 instances). After that was the suggestion to use software to block automated processes on websites such as pop-ups and scripts which had 5 recommendations. Finally, was to use a sandbox software to open suspicious files which appeared 3 times in the coding.

Two other techniques were commonly suggested—Target Hardening and Controlling Access to Facilities (a.k.a. controlling access to the computer). About 12% of all advice mentioned techniques that could be classed as target hardening. Of note within the 45 codings, the most frequently mentioned tactic was installing anti-virus or anti-malware programs with 22 instances. Other examples within this technique are:

- “Install Adaware”
- “Install a good Antivirus/Anti-spyware”
- “spend a few bucks on a good anti-spyware program”

Not as common, but worth mentioning were the 30 instances of advice falling within the technique, controlling access to facilities (8% of all coding). The

two most noteworthy recommended strategies were to use a firewall with 8 instances and use a password with 5 instances. Examples of other advice in this category include:

- “Restricted Connectivity”,
- “Enabling HTTPS for all logins and wp-admin”,
- “Restrict Direct Access to Plugin and Theme PHP files”

The remaining five suggestions were coded as Control tools (1%) or Screen exits (.2%). Examples follow:

- Control Tools:
  - “Restrict administrative privileges to operating systems and applications based on user duties”
  - “Don't make someone teach u hacking,better learn by urself.”
- Screen exits:
  - “first thing you should do is spoofing your mac-address.”

Increase the Risks

Within this category were 11% of the total coding within this category were first Utilize Place Managers that had 4% of the total coding. The strategies of note were to use third-party websites to examine web traffic with 6 instances. This was followed by using a third-party website to look for flaws inside of a server and to use Virus Total to scan files before opening them with 3 and 2 respectively. Some other recommendations include:

- “Download from known sites”,
- “Use two factor authentication as much as possible.”,
- “Scan suspicious files using VirusTotal before downloading it”

Next, was Strengthen Formal Surveillance with 3% of the total coding. Within this category the most frequently recommended strategy was to run some sort of scan on your important files with 8 instances. Other examples of advice are:

- “Scan your PC once a week”,
- “First and foremost, you don’t want to limit yourself to one antivirus program.”,
- “Perform an endemic test at the documents/e-mail attachments which you down load before executing them.”

After that, the next category with coding was Extend Guardianship with 2% of the total coding. Of note within this category is that the hacking community suggested to regularly check any activity on important data. Other examples of this category include:

- “Before opening a program always scan it”,
- “take a look at the list of applications installed on your smartphone. If you notice a dubious application, get rid of it right away”
- “Always Check the URL in the Address Bar”

Finally, in this category was Assist Natural Surveillance with .7% of the coding examples of which are:

- “Always type the URL of the site in the address bar to get into the site. Do not click on a hyperlink to enter the site”
- “The best way to defend against the “Trusted Contact” Facebook scam is to contact the friend directly. Not by email or text, make sure it is in person or at least over the phone”

Reducing Rewards

It was found that the category used most by the hacking community was Reducing Rewards with 46% of the total coding. Within this category the most prevalent technique was Remove Targets at 27%. Within this technique not clicking on suspicious links is the most recommended strategy with 11 instances found within the coding’s. The next strategy most recommended is to not use public computers/Wi-Fi with 10 instances. After that, is to only visit secure and trusted websites and do not download or click on suspicious emails with 7 instances each. The last strategy recommended of note is to not install plug-in and toolbars onto your browser with 5 instances. Some other examples of remove targets are:

- “Do not click on unsolicited email”
- “Don’t install toolbars”
- “Do not click on popups”

- “NEVER double-click the pen drive to open it. Instead right-click on it and select the option ‘open’”
- “Secondly, don’t click on a link in an email or social media message that sounds suspicious.”

Next, was Conceal Targets which had 18% of the coding’s. Within this category the strategy most recommended was use a VPN when browsing the internet which had 23 instances. After that, the next strategy that was recommended was to encrypt your data with 13 instances. Next, with 7 instances inside of the coding’s was to use a Virtual Machine on your computer. The final two strategies recommended with 5 instances each are use an anonymous browser like Tor and use a password management software. Some other examples of this technique are:

- “disable the on- screen SMS previews”,
- “Encrypt Your Wireless Router Connection”,
- “Never Put Author Usernames on Display”

Finally, the last represented technique is Deny Benefits with 1% of the total coding. Examples of this include:

- “keeping around a known-good firmware image and wiping your hard drive + reflashing the firmware every month.”
- “Android Device Manager”

Reduce Provocation

This category contained 9% of the total amount of coding. Within this category was Discourage Imitation with 8% of the sample. Within this category the most recommended strategy, both inside the technique and in the entirety of the sample, was to keep your software and devices updated with 30 instances. Recommendations include:

- “It is highly recommended that you turn on the automatic update feature”,
- “Install Updates Frequently”,
- “Patch everything, immediately.”

Next, was Reduce Emotional Arousal with 1% of the coding, examples include:

- “Revert the SSO system back to OAuth 2”
- “Change your default passwords.”

Finally, at .5 percent was Avoid Disputes examples of which are:

- “Don't try to hack others”
- *“Change your default passwords.”*

The category Remove Excuses were not represented within the coding.

Level of Expertise

Q2. What level of expertise is the advice recommended by the hacker community geared towards?

It was found that most of techniques were being recommended for those with novice levels of computer knowledge. There was a total of 77 out of the 85 pages that contained strategies that could be used by those with novice levels of computer knowledge. On the other hand, expert level of advice was only found on 21 out of the 85 pages. Novice also comprised 90% of the total codings. Some examples of these types of codes are:

Novice:

- “You also need multiple passwords for all your accounts and never share critical software passwords with non-critical software”,
- “Scan your PC once a week”,
- “Secure your mobile phone with a password or with another method such as fingerprint recognition but do not unlock it when it is in charging”,
- “Always install a terrific antivirus software program”

Expert:

- “Resolve the subdomain takeover of saostatic.uber.com by removing the dangling CNAME to AWS CloudFront CDN”,
- “Restrict Access to wp-admin Directory”,
- “Make a // entry in config.php that displays the WordPress table prefix used in the installation”,
- “Filter MAC Addresses”

CHAPTER FIVE

DISCUSSION

Examining the results, three themes emerge from this study. These themes include: hacker opportunities, routine protections, and finally, the difficulty encountered in applying the Situational Crime Prevention framework when coding recommendations. The first theme that will be presented is on hacker opportunities. This section will first, cover the motivations of the typical hacker. Next, this section will present how studying hacker opportunities can be used to protect victims. Finally, this section will cover how the limitations of this study could influence the results, along with where future research should focus.

The second theme that will be discussed is Routine Precautions. First, this section will talk about what Routine Precaution theory posits and how that is related to internet crime. Next, this section will address what Felson and Clarke (2010) suggest to encourage people to take the correct routine precautions. After that, this section will go over the routine precautions that are shown from the results of this study. Finally, limitations to this project, as well as, areas for future research will be presented.

The last theme this chapter will cover are the difficulties in applying Situational Crime Prevention. This first part of this section will go over what areas of SCP were not represented in the results of this study. This section then proceeds to go over why internet crimes might not fit within the SCP framework.

Finally, this section will go over how the limitations in coding could have caused this and how future research might solve this problem.

Hacker Opportunities

While the image of large scale hacking groups breaking into sophisticated security systems dominates the media, the results of this study suggest that hackers are not wary of sophisticated attacks. By examining the protection strategies recommended by the hacking community a clear theme emerges. This theme reveals that hackers are not concerned by highly-skilled hacking, but small scale, simple opportunistic hacking. The advice featured in the hacking community recommendations focuses on common sense protection methods, not complicated security practices. For example: patching software, not clicking on suspicious items, and running virus scans on files before opening them are all advice that thwart those hackers who are relying on human mistakes to carry out their attacks. This is further shown by the fact that 90% of all strategies recommended could be used by those with novice levels of experience.

These findings are indirectly supported by several studies investigating hacker motivations. First, a survey performed by the security company Thycotic (2014) revealed, in their sample of 127 self-identified hackers attending a hacking conference, that 51% of the hackers said that they hacked for the fun and thrill of hacking. This finding is also supported by research conducted by Madarie (2017). In their study they administered a survey to 71 self-identified hackers to figure out the underlying motives behind why they hack. Part of their

findings suggested that hackers rated intellectual challenge and curiosity as the highest motivational factor behind why they circumvent security systems. This is followed by peer recognition and respect. The least rated motivational factor hackers rated was money. While Madarie also found that these motivating factors did not determine how often they participated in hacking, it does suggest that hacking to go after large sums of money from their victims is rare. Finally, Turge-GoldSchmidt (2005) interviewed 54 Israeli hackers as to why they hack and found that the most stated motivating factor for their hacking activities was fun, thrills, and excitement. In their interviews only one hacker said that economic reasons were why they hacked. So the most immediate threat is posed by opportunistic thrill seekers, no bands of committed and highly-skilled criminal entrepreneurs motivated by profit goals.

Policy Implications

The findings in this study suggest that hackers are not concerned with sophisticated attacks on their systems. Drawing upon Seebruck's (2015) updated typology of hacker, and in consideration that most hackers act out of a desire for thrill and excitement rather than profit, the results of the current study suggest that hackers are more concerned with the threats posed by opportunist and recreational hackers. These are the hackers who do so for the fun and thrill of exploiting a mistake someone makes in their browsing habits. To combat this, users should forget about the dramatized vision of the hackers who break through the toughest of security to steal their data. This mentality leads to users

thinking that there is nothing they can do to prevent them getting their personal information. This is false, as the most recent Thyoctic (2017) survey shows, 85% of the hackers agreed that most data breeches are caused by human error. This shows there must be a shift in thinking that hacking is inevitable to hacking can be prevented with the right precautions taken.

Limitations

There are some limitations to this project that could interfere with the conclusions drawn from this theme. The most important of which is that there is no way to assess the effectiveness of each strategy, proving the strategy was deployed correctly. Because of this, this project can only make assumptions based on the prevalence of each strategy recommended.

Future Research

Future research should examine the effectiveness of these techniques to determine if the recommended prevention strategies are in fact, the most effective ways of preventing cybertheft. This would allow researchers to say for certain that these strategies are effective for stopping opportunistic hackers. Future researchers should also interview hackers about their safety concerns. This would then reveal what are the exact fears that hackers have when browsing online.

Routine Precautions

> Suppose all situational controls were abandoned: no locks, no custom controls, cash left for parking in an open pot for occasional collection, no library checkouts, no baggage screening at airports, no ticket checks at train stations, no traffic lights, etc. Would there be no change in the volume of crime and disorder? (Tilley and Laycock, 2002:31).

The above quote ties into the second theme that can be drawn from the findings. This theme is tied to the theory of routine precautions. This theory, developed by Felson and Clarke (2010), posits that throughout our lives we naturally take precautions against crime. For example, locking doors, avoiding certain places, and staying inside at night are all precautions that many take without thinking. Felson and Clark suggest that this theory is another important aspect in the prevention of crime.

Felson and Clark state that society is governed by three forms of control: informal, formal, and routine precautions. Informal control is where society helps to control crime. For instance, if someone strange enters the neighborhood and starts to mess with a person's car and that person's neighbor intervenes to either stop the perpetrator, or call the neighbor to explain the situation. Formal control is the criminal justice system that seeks to prevent these types of crimes from

happening. Finally, there are the routine precautions that each citizen takes to prevent their own victimization.

Felson and Clarke (2010) argue that some global social trends are weakening informal and formal controls. For example, in today's society people are strangers to one another thus weakening the informal controls. Furthermore, advances in technology help criminals become more anonymous weakening formal controls. Felson and Clarke (2010) suggest that these declines in informal and formal controls will lead to the rise in routine precautions. Felson and Clark also speculate that through the rise in technology these declines will happen faster. This can clearly be seen with the technological advances brought about by the internet. With the internet there are few informal controls that can stop someone from becoming a victim of identity fraud or some other crime. Moreover, law enforcement is powerless to stop most forms of internet crime because of the private nature of the internet, thus eroding the formal control.

Felson and Clarke claim that there is a need to address the specific situation of crime. This means to focus not on why offenders commit crimes, but on what situations allow offenders to commit those crimes. What then, are the situations where internet crime takes place? While this study did not cover the situations where these crimes take place there can be inferences drawn from the results of what hackers recommend. For instance, the most recommended strategy was to keep your software updated. This reveals that many hackers are breaking through outdated software.

As shown through the findings of this research, much of the advice given relies on users taking more precautions against shady practices. While the advice given sounds as obvious as, locking our car doors at night or avoiding bad parts of town; it is still a fact that millions of people could have avoided victimization by simply not clicking on the link or downloading a file. It may be the case that simple, routine precautions, such as knowing that if you click on those links or download those files you will be infected with a computer virus that steals your credit card information, are not in common use.

The next question to ask is, what then would need to be done to adopt routine precautions against internet crime? Felson and Clarke (2010) speculate that it would be easier to get organizations and governments involved with getting people to adopt routine precautions then getting citizens themselves to adopt them

> It is easier to change the minds of a few thousand organizations than to change the minds of 250 million individuals. By working with organizations rather than individuals, it may be possible to bring prevention to fruition more quickly while feeding back what is learned into improved criminology. (pg. 118)

Policy Implications

Felson and Clarke conclude that governments will increasingly rely on routine precautions to prevent crime. They state that there are multiple items that

governments will need to consider: the range and prevalence of routine precautions, the public and private resources, their inconvenience and opportunity costs, their effectiveness and efficiency as crime prevention measures, and their other benefits from feelings of empowerment and control. Once governments are onboard with promoting routine precautions, then the challenge becomes getting citizens to adopt these routine precautions. Felson and Clark go on to posit five methods to convince citizens to adopt routine precautions--formal social controls, informal supervision, signage and instructions, product design to facilitate routine precautions, and finally design to improve natural surveillance.

(1) Formal social controls are laws designed to protect citizens such as curfews. When applied to internet crimes this would be mandating important websites and software to force users to change their passwords to thwart people from compromising their passwords.

(2) Informal supervision is when people keep an eye out for each other. This could include family members watching for criminal activity. As well as, reminding their friends and family to lock up and other tips to keep them safe. This could be used on internet crimes by reminding family members to not go to suspicious links and to update their computer software.

(3) Signage and instructions is when there are notes and signs posted around a neighborhood or areas where people travel. For instance, the signs you see reminding you to lock your car doors. Another example is the signs around

Barcelona warning tourists about pick pockets. Applying this strategy to the internet this would be like email services displaying messages not to download attachments from unknown senders.

(4) Products designed to facilitate routine precautions would include lockers with automated locks where users can choose their own password. Another example would be cars that lock automatically a short while after the key has been removed. An example of this in the internet world would be computers that automatically update their software.

(5) Finally, are designs that improve natural surveillance. This would include installing motion lights or making sure that dark areas around their house are illuminated. In the internet this would be installing anti-virus on a computer or a website that hosts files scanning the files before they are made public.

After seeing how these routine precautions can be applied to the public one can then ask what precautions should be endorsed. Felson and Clarke (2010) recommend that routine precautions are grouped into bundles that are proven to work. This avoids overloading the population with precautions that do not work or contradict each other. Examining the results of this study, there are multiple strategies that can be bundled together. Seven strategies that can be derived from the results to be routine precautions include: Do not click on suspicious links, do not use public Wi-Fi/computers, install antivirus/antimalware, use strong unique passwords, run scans on important files, check activity on important data, and finally keep software updated.

These strategies, if implemented by the public, could be instrumental in combatting the wave of internet crime and personal data breeches. Although these strategies did not come from examining citizens routine precautions, it is important to note that that they did come from the hacking community. As Jacques and Reynald (2012) stated there is a need to learn from offenders to protect ourselves. Furthermore, Thycotic (2014) found that 88% of hackers surveyed believe their information is at risk. Therefore, these precautions should be considered as routine precautions. This is because if hackers are concerned about their personal information being at risk, then everyone who accesses the internet is at risk as well.

Limitations

While these strategies were recommended by the hacking community, as stated before, there was no data to suggest how effective each strategy was in preventing crime. Additionally, this project sought to capture more in scope. For example, this project sought to capture the dates of technique recommended to see if techniques changed over time, however data on this was not collected in the data gathering process so that fell outside of the scope of this project. This means there is no way to tell if the strategies recommended change over time. Additionally, this project sought to gather exposure data and data from videos, but there was not enough information on those categories to put into this project. This could have given more information about the effectiveness of the strategies.

Finally, when examining fan pages, the only website looked at was Reddit which could have influenced these recommendations.

Future Research

Future studies should look at how effective these strategies are in reducing crimes. As Felson and Clarke (2010) called for, bundles of routine precautions should be examined for their effectiveness. Also, future researchers should look at how feasible it is to educate the general population about these strategies and to make these strategies routine precautions. Finally, future research should look at different forms of hacker media and interview hackers to come up with more accurate routine precaution bundles.

Difficulties in Applying Situational Crime Prevention

While situational crime prevention has had success in being applied to offenders as victims of conventional street crime (Jacques & Reynald, 2012) and to cybercrime generally (Hinduja & Kooi, 2013; Willison & Siponen, 2009), the final theme emerging from the present study is that the SCP lens was not fully realized when applied to cybertheft. For example, while Jacques and Reynald (2012) found in their study of offenders use of SCP that their sample of drug dealers used all the main categories of SCP, this study found that hackers did not. There were no prevention strategies identified for any of the categories of Remove Excuses. Even within the most represented category, Reduce the Rewards, there are still specific techniques categories with no representation in all of the 379 codings, i.e., identify property and disrupt markets had zero codings

tied to those techniques. Another technique that was not represented within the coding was the reduce anonymity technique in the category Increase Effort. Finally, in the category of Reduce Provocation, I found no recommendations of techniques to reduce frustration and stress and neutralize peer pressure.

Furthermore, research looking at applying SCP to the information security sector had similar struggles of applying SCP. Looking back at research by Willison and Siponen (2009), they sought ways to apply the 25 techniques of SCP to information security. They produced a modified SCP chart that had examples from the information security world. However, this chart did not have any examples for the techniques Disrupt Markets, Avoid Disputes, Reduce Emotional Arousal, Neutralize Peer Pressure, Post Instructions, Alert Conscience, and finally Control Drugs and Alcohol. Willison and Siponen argued that these techniques that did not have examples were areas to be looked at further by practitioners. Yet, as this research shows, those areas might prove difficult to fully explore with SCP. Other SCP research on information security has had success in applying SCP to that area but with modifications to the current table. Hinduja and Kooi (2013) managed to apply the techniques of SCP to information security by using the original 16 techniques instead of the current 25. Hinduja and Kooi deemed the original iteration of SCP to be more appropriate for information security because it has more generalizability than the techniques used presently.

Looking at these results from this study, the majority of categories and techniques that did not show in the findings were those that rely on personal interactions. One reason for this is because cybertheft does not rely on personal interactions. For example, infecting someone's computer with a virus to steal their information could easily be done through an infected link sent out to random people online. So, while there are multiple studies showing that SCP can prevent street crime (Anderson & Pease, 1994; Challinger, 1996; Clarke, 1990; Matthews, 1990), the present study suggests that SCP might not be fully applicable to specific types of online crimes.

Limitations

This study does have important limitations that can contribute to these results. Most importantly, the strategies recommended were classified under a specific technique using a best fit protocol. What this means is that if a strategy did not fit well under one of the five techniques it was placed into one that seemed to be the best fit. Also, if a strategy could be classified as several different techniques, I used my best judgement to classify it as one technique. What this means is that some strategies were placed into their categories subjectively therefore someone else might say that those strategies could be placed into other techniques.

Future Studies

Future studies should first, come up with a guide on how to classify strategies to techniques. This would allow researchers to avoid biases in coding,

as well as, confusion when encountering unknown strategies that do not fit within any technique or category. Moreover, future studies should examine only categories of SCP as that would allow the classifying of strategies to be less confusion about which strategies go to which techniques.

Conclusion

This project examined the protection methods suggested by hackers to guard against online victimization through the lens of Situation Crime Prevention. The data were collected from 85 webpages representing three categories of electronic communications: forums, blogs, and fan pages. The goal of this project was to identify which of the 25 opportunity reduction techniques the hacking community recommend most often, as well as, what level of expertise is associated with the suggested security measures. Results indicated that the technique most recommended by the hacking community was remove targets with 27% of the total codings. Results also showed that 90% of all advice given could be used by those with little computer knowledge.

From the results three themes emerged: hacker opportunities, routine precautions, and finally, the difficulties in applying SCP. It was found that the hackers are not overly concerned with professional, highly-skilled attacks, rather their advice would thwart recreational opportunists. The results also showed support for Routine Precautions theory which states that we all take routine precautions against crime every day. It is speculated that because the internet is new, these routine precautions are not ingrained within the general population, therefore cyber-oriented suppliers should be pressured into building routine precautions into their products. Finally, it was found that SCP had limitations on how it could be applied to stop cybertheft, in part because this class of crime does not always require direct victim-offender interaction. This was shown in

other research which also had difficulties in applying the techniques of SCP. This study demonstrates that much can be learned that will advance cybercrime prevention from the listening to the offenders themselves.

APPENDIX A

LIST OF SOURCES

LIST OF SOURCES

Type	Site	Links	# of pages
Forums	Hack Forums	https://hackforums.net/	19
Forums	Offensive Community	http://offensivecommunity.net/	1
Fan Pages	r Ask Nec Sec	https://www.reddit.com/r/AskNetsec/	2
Fan Pages	r Hacking	https://www.reddit.com/r/hacking/	10
Fan Pages	r Hacking Tutorials	https://www.reddit.com/r/Hacking_Tutorials/	1
Fan Pages	r How to Hack	https://www.reddit.com/r/HowToHack/	4
Blog/Static	arneswinnen	https://www.arneswinnen.net/	1
Blog/Static	Coding Horror	https://blog.codinghorror.com/hacker-hack-thyself/	1
Blog/Static	Criminalscity	http://criminalscity.blogspot.com/	6
Blog/Static	Dark Cyber Society	http://www.darkcybersociety.com/	1
Blog/Static	Darknet	https://www.darknet.org.uk/	2
Blog/Static	Effect Hacking	http://www.effecthacking.com/	4
Blog/Static	ehacking	https://www.ehacking.net/	1
Blog/Static	extreme hacker	http://blog.extremehacking.org/	2
Blog/Static	Graceful Security	https://www.gracefulsecurity.com/	1
Blog/Static	Hack Read	https://www.hackread.com/	2
Blog/Static	hackers online club	https://blog.hackersonlineclub.com/	4
Blog/Static	Hacking Tutorials	https://www.hackingtutorials.org/	4
Blog/Static	itechhacks	https://itechhacks.com/	2
Blog/Static	Latest Hacking News	https://latesthackingnews.com/	6
Blog/Static	official hacker	https://www.officialhacker.com/	3
Blog/Static	Pure Hacking	https://www.purehacking.com/blog	1
Blog/Static	The Hacker Blog	https://thehackerblog.com/	3
Blog/Static	The Hacker News	https://thehackernews.com/	4

REFERENCES

Adler, F., Mueller, G. O., & Laufer, W. S. (2010). *Criminology*. New York: McGraw-Hill Higher Education.

Alfred Ng, Steven Musil. (2017, September 07). Equifax data leak may affect nearly half the US population. Retrieved November 09, 2017, from https://www.cnet.com/news/equifax-data-leak-hits-nearly-half-of-the-us-population/

Anderson D., Chenery S. and Pease, K. 1994. *Preventing Repeat Burglary and Car Crime*. Crime detection and prevention paper 58, London: Home Office

Andresen MA, Felson M (2010). Situational crime prevention and co-offending. *Crime Patterns Analysis* 3(1):3–13

Barratt, M. J., Lenton, S., Maddox, A., & Allen, M. (2016). 'What if you live on top of a bakery and you like cakes?'—drug use and harm trajectories before, during and after the emergence of silk road. *International Journal of Drug Policy, 35*, 50-57. doi:10.1016/j.drugpo.2016.04.006

Bazeley, P. (2002). The evolution of a project involving an integrated analysis of structured qualitative and quantitative data: From N3 to NVivo. *International Journal of Social Research Methodology, 5*(3), 229-243.

Beauregard, E., Leclerc, B., & Lussier, P. (2012). Decision making in the crime commission process. *Criminal Justice and Behavior, 39*(10), 1275-1295.

Bérubé, H. (2010). An examination of alarm system deterrence and rational choice theory: The Need to Increase Risk. *Journal of Applied Security Research, 5*(3), 326-381.

Breetzke, G. D., & Cohn, E. G. (2013). Burglary in gated communities. *International Criminal Justice Review, 23*(1), 56-74. doi:10.1177/1057567713476887

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology, 8*(1), 1-20.

Challinger, D. (1996). Refund fraud in retail stores. *Security Journal* 7: 27-35

Choo, K. R. (2008). Organized crime groups in cyberspace: a typology. *Trends in Organized Crime, 11*(3), 270-295. doi:10.1007/s12117-008-9038-9

Clarke, R. V. (1990). Deterring obscene phone callers: preliminary results of the new jersey experience. Security Journal 1: 143-148.

Clarke, R. V. (2010). *Situational crime prevention: successful case studies*. Boulder: Lynne Rienner .

Clarke, R., & Cornish, D. (1985). Modeling offenders' decisions: a framework for research and policy. *Crime and Justice, 6*, 147-185.

Crowley, C., Harre, R., & Tagg, C. (2002). Qualitative research and computing: methodological issues and practices in using QSR NVivo and NUD*IST. *International Journal of Social Research Methodology, 5*(3), 193-197. doi:10.1080/13645570210146258

Dickinson, T., & Wright, R. (2015). Gossip, decision-making and deterrence in drug markets. *British Journal Of Criminology, 55*(6), 1263-1281.

Dogaru. (2012). Criminological characteristics of computer crime. *Journal of Criminal Investigations, 5*(1), 92-98.

Dovidio, R. (2007). The evolution of computers and crime: complicating security practice. *Security Journal, 20*(1), 45-49.

Doyle, C. (2013). *Cybercrime: an overview of the federal computer fraud and abuse statute and related federal criminal laws*. Lexington, KY: Congressional Research Service.

Dupont, B., Côté, A., Savine, C., & Décary-Hétu, D. (2016). The ecology of trust among hackers. *Global Crime,* 1-23.

Ekblom, P., & Tilley, N. (2000). Going equipped: Criminology, situational crime prevention and the resourceful offender. *The British Journal of Criminology, 40*(3), 376-398.

Felson, M., & Clarke, R. V. (2010). Routine precautions, criminology, and crime prevention. In *Criminology and Public Policy* (pp. 106-120). Philadelphia, PA: Temple University Press.

Grabosky, P. N. (2001). Virtual criminality: old wine in new bottles? *Social & Legal Studies,10*(2), 243-249. doi:10.1177/a017405

Hinduja, S., & Kooi, B. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. *Security Journal, 26*(4), 383-402.

Holt, T. J., & Bossler, A. M. (2013). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20-40. doi:10.1080/01639625.2013.822209

Hutchison, A., Johnston, L., & Breckon, J. (2010). Using QSR-NVivo to facilitate the development of a grounded theory project: an account of a worked example. *International Journal of Social Research Methodology, 13*(4), 283-302.

IC3 ... Internet crime report. (2016). Washington, D.C.: National White Collar Crime Center.

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice, 47*, 44-57. doi:10.1016/j.ijlcj.2016.07.002

Jacques, Allen, & Wright. (2014). Drug dealers' rational choices on which customers to rip-off. *International Journal of Drug Policy, 25*(2), 251-256.

Jacques, S., & Reynald, D. M. (2011). The offenders' perspective on prevention. *Journal of Research in Crime and Delinquency, 49*(2), 269-294. doi:10.1177/0022427811408433

Johnston, L. (2006). Software and method: reflections on teaching and using qsr NVivo in doctoral research. *International Journal of Social Research Methodology, 9*(5), 379-391.

Kshetri, N. (2016). Cybercrime and cybersecurity in india: causes, consequences and implications for the future. *Crime, Law and Social Change, 66*(3), 313-338.

Leukfeldt, E., Kleemans, R., & Stol, E. (2017). A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change, 67*(1), 21-37.

Leukfeldt, E., Lavorgna, A., & Kleemans, E. (2017). Organised cybercrime or cybercrime that is organised? an assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research, 23*(3), 287-300.

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: overview and issues. *Crime, Law and Social Change, 67*(1), 3-20.

Louderback, E., & Antonaccio, O. (2017). Exploring cognitive decision-making processes, computer-focused cyber deviance involvement and victimization. *Journal of Research in Crime and Delinquency, 54*(5), 639-679

Loughran, T., Paternoster, R., Chalfin, A., & Wilson, T. (2016). Can rational choice be considered a general theory of crime? evidence from individual-level panel data. *Criminology, 54*(1), 86-112.

Madarie, R. (2017). Hackers' motivations: testing Schwartz's theory of motivational types of values in a sample of hackers. *International Journal Of Cyber Criminology*, *11*(1), 78-97. doi:10.5281/zenodo.495773

Matthews, R. (1990). Developing more effective strategies for curbing prostitution. *Security Journal* 1:182-187

McCarthy, B. (2002). New economics of sociological criminology. *Annual Review of Sociology, 28*, 417-442.

Moloney, M., Hunt, G., & Joe-Laidler, K. (2015). Drug sales, gender, and risk: notions of risk from the perspective of gang-involved young adults. *Substance Use & Misuse, 50*(6), 721-32.

Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimization among young people: a multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention,* 1-8.

Paternoster, R., & Pogarsky, G. (2009). Rational choice, agency and thoughtfully reflective decision making: the short and long-term consequences of making good choices. *Journal of Quantitative Criminology, 25*(2), 103-127.

Paulus, T., Woods, M., Atkins, D., & Macklin, R. (2015). The discourse of QDAS: reporting practices of ATLAS.ti and NVivo users with implications for best practices. *International Journal of Social Research Methodology,* 1-13.

Piliavin, I., Gartner, R., Thornton, C., & Matsueda, R. (1986). Crime, deterrence, and rational choice. *American Sociological Review, 51*(1), 101-119.

Piza, E., & Sytsma, V. (2016). Exploring the defensive actions of drug sellers in open-air markets. *Journal of Research in Crime and Delinquency, 53*(1), 36-65.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 267-296. doi:10.1177/0022427810365903

Rege-Patwardhan, A. (2009). Cybercrimes Against Critical Infrastructures: A study of online criminal organization and techniques. *Criminal Justice Studies, 22*(3), 261-271.

Seebruck, R. (2015). A typology of hackers: classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation, 14*, 36-45.

Sullivan, C. (2009). Is identity theft really theft? *International Review of Law, Computers & Technology, 23*(1-2), 77-87.

Taylor, E. (2014). Honour among thieves? how morality and rationality influence the decision-making processes of convicted domestic burglars. *Criminology & Criminal Justice, 14*(4), 487-502.

That's three billion accounts -- including email. (n.d.). Every single Yahoo account was hacked. Retrieved November 09, 2017, from http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html

Tilley N, Laycock G: *Working out what to do: Evidence-Based Crime Reduction. Crime Reduction Research Series Paper 11*. Home Office, London; 2002.

Townsley, M., Birks, D., Ruiter, S., Bernasco, W., & White, G. (2016). Target selection models with preference variation between offenders. *Journal of Quantitative Criminology, 32*(2), 283-304.

Turgeman-Goldschmidt, O. (2005). Hacker's accounts. *Social Science Computer Review, 23,* 8-23.

Wall, David S. (2001). Cybercrimes and the internet. Pp. 1–17 in Crime and the Internet, edited by David S. Wall. New York: Routledge.

Ward, D., Stafford, M., & Gray, L. (2006). Rational choice, deterrence, and theoretical integration. *Journal of Applied Social Psychology, 36*(3), 571-585.

Wortley, R., & Townsley, M. (Eds.). (2016). *Environmental criminology and crime analysis*. Retrieved from https://ebookcentral.proquest.com

Webb, B. (1994). Steering column locks and motor vehicle theft: evaluation from three countries. In R. V. Clarke (ed), *Crime Prevention Studies*, Vol. 5. Monsey, NY: Criminal Justice Press

Weise, E. (2015, October 01). Experian breach may have exposed 15 million T-Mobile records. Retrieved November 09, 2017, from https://www.usatoday.com/story/tech/2015/10/01/t-mobile-breach-may-have-exposed-15-million-records/73171066/

Wilcox, Pamela, Gialopsos, Brooke Miller, Coyne, Michelle A, & Eck, John E. (2015). Situational choice and crime events. *Journal of Contemporary Criminal Justice, 31*(1), 12-29.

Willison, R., & Siponen, M. (2009). Overcoming the insider: reducing employee computer crime through situational crime prevention. *Communications of the ACM, 52*(9), 133-137.

Yoon, Sungwon, Lam, Wendy W.T., Sham, Judy T.L., & Lam, Tai-Hing. (2015). Learning to drink: How Chinese adolescents make decisions about the consumption (or not) of alcohol. *International Journal of Drug Policy, 26*(12), 1231-1237.

Zetter, K. (2009, September 09). ‘Anonymous’ declares war on Australia over internet filtering. Retrieved November 09, 2017, from https://www.wired.com/2009/09/anonymous-hacks-australia/