Copyright © 2019 International Journal of Cyber Criminology – ISSN: 0974–2891
January – June 2019. Vol. 13(1): 101–116. DOI: 10.5281/zenodo.3551489
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

Guarding against Cyber-Trespass and Theft: Routine Precautions from the Hacking Community

Nicholas Chavez[1] **& Gisela Bichler**[2]
California State University San Bernardino, United States of America

Abstract

Positing that hackers are attuned to the risks and vulnerabilities of online activity, this study used the situation crime prevention (SCP) framework to examine the protection methods promoted within hacking forums to guard against online victimization. Data were collected from 85 webpages representing two categories of electronic communications: forums and blogs. Three goals drove this project: 1) to investigate whether the set of recommendations fit the SCP framework; 2) to identify what opportunity reduction techniques were most often recommended by the self-identified hacking community; and, 3) to examine the level of expertise associated with the suggested security measures. Strategies aimed at increasing the effort required to commit crimes, and reducing the rewards associated with cyber-trespass and theft, figured prominently—the specific strategy most recommended was to keep computer software updated. Ninety percent of recommendations require minimal computer skills. Continued efforts are needed to explore the utility of asking potential offenders for advice when developing recommendations on routine precautions that people could use to protect themselves online.

Keywords: Situational Crime Prevention, SCP, Cyber-Theft, Cyber-Trespass, Routine Precautions, Hacking.

Introduction

Inundated with reports of major data breaches exposing the private information of millions of people, it is hard to ignore issues of security in a digital age. Cyber crime is a broad class of behavior that includes any crime occurring on, or using a computer. Encompassing 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, cyber criminology is a rapidly developing field (Dogaru,

[1] Research Assistant, Department of Psychology, California State University, San Bernardino, 5500 University Parkway San Bernardino, CA 92407, USA. Email: nchavez42100@gmail.com

[2] Professor and Director, Department of Criminal Justice, California State University, San Bernardino, 5500 University Parkway San Bernardino, CA 92407, USA. Email: gbichler@csusb.edu

2012; Doyle, 2012; D'Ovidio, 2007, Holt & Bossler, 2014; Jaishankar, 2009, 2018; Kshetri, 2016; Ngo & Jaishankar, 2017; Nasi, Oksanen, Keipi, & Rasanen, 2015).

Cybercrime is disruptive and costly. Estimates suggest that in the United States losses surpass a billion dollars annually, i.e., 1.33 billion dollars in 2016 as reported by the Internet Crime Complaint Center (IC3 2016). Global estimates show that the 2017 estimated cost of cybercrime was over 600 billion dollars (McAfee, 2018).Since these figures reflect only reported crime and estimates do not generally include the losses people incur when trying to reestablish credit, reinstate their identity, or secure their systems, the true harm of cybercrime is significantly higher. As with conventional types of crime, 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).

With the speed with which internet-based technology is inundating all facets of life, and the growing magnitude of personal information that is being systematically captured and stored in electronic systems, there is a vital need for criminological research into computer crime (Willison & Siponen, 2009), particularly, studies which examine this phenomenon from the offenders' perspective. Learning more about what offenders perceive to be vulnerabilities help us to understand how to diagnose system weaknesses and prevent crime. Why? Because the people who commit the crimes have a significant advantage—they are best positioned to identify the mechanisms most apt to prevent themselves from successfully committing a crime (e.g., Cromwell & Nielson, 1999; Decker, Wright, & Logie, 1993; Jacques & Reynald, 2012). With this knowledge, there is the prospect of invoking crime prevention measures that significantly influence offenders' decision making (e.g., Decker et al., 1993)

The focus of the present study is on preventing the related crimes of *cyber-theft* and *cyber-trespass,*[3] as these two types of crime are linked to the majority of cyber crime losses. *Cyber-theft* involves activities used to obtain an individual's information, such as their social security or credit card numbers, and then, using the information on the internet to commit other crimes, i.e., identity theft, purchasing goods, and buying illicit products [Holt and Bossler (2014) expanding on Wall (2001)]. Use of computers is not a necessary condition for procuring personal information: personal information can be obtained from hardcopy documents that are discarded in the trash, through deception, or breach of trust (e.g., from documents viewed at work). While the initial theft of personal data does not

[3] Expanding upon Wall's (2001) categories of cyber crime, Holt and Bossler (2014) developed a classification scheme using four categories. (1) *Cyber-trespassing* includes 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. (2) C*yber-porn and obscenity* involves using the internet to acquire videos or pictures, arrange for the production or dissemination of illicit material, or solicit illicit sex. (3) *Cyberviolence* includes assaultive behavior that targets individuals (e.g., cyber stalking, harassment, or threats of violence online) and assaultive behavior targets organizations and systems (e.g., 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). (4) *Cyber-deception and theft* involves acquiring 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.

necessarily require advanced computer skills, or even the use of computers, some theft does. Another related type of crime, and possible precursor crime to cyber-theft, is *cyber-trespassing*. Cyber-trespassing involves accessing computer infrastructures that do not belong to the individual, i.e., hacking into secure systems. Estimates suggest that about half of the theft-related losses to cybercrime involve some form of cyber-trespass [e.g., an IC3 (2016) report shows that hacking related losses in 2016 were estimated to be about 527 million dollars].

The current study investigates security advice to protect against cyber-trespassing and theft that is circulated within self-identified hacking communities. Three objectives drive this inquiry. (1) We catalogue and indirectly capture the confidence placed on measures recommended by the hacker community by tallying the number of times a technique is mentioned. (2) By investigating how recommendations fit within the situational crime prevention (SCP) framework, we assess the utility of using this classification system when considering offender perspectives. And, (3) we examine the level of expertise associated with the suggested security measures to understand whether recommended prevention strategies can be incorporated into the average person's routine precautions. In what follows, we review the framework used for this study, explain the qualitative methods used, and describe the main themes that emerge. Finally, we discuss the policy and research implications of what we learned about hacking opportunities, the feasibility of recommended routine protections, and the difficulties associated with applying the SCP framework.

Understanding Target Vulnerabilities

1. Situational Crime Prevention

Proponents of SCP advocate developing a set of strategies to remove the opportunities for crime, in part, by increasing the disadvantages of committing a crime (Clarke, 2010). It is reasoned that increasing disadvantages over anticipated rewards would lead potential offenders to refrain from committing a specific crime—influencing the rational decision-making process could prevent crime. To be effective, Clarke (2010) suggests that the opportunity-reducing measures must: (1) be directed at a specific form of crime; (2) involve a change in an environment that is as permanent as possible; and, (3) make crime riskier to the offender or provide the offender with less reward. SCP does not seek to explain crime, rather, the object is to facilitate the implementation of prevention strategies that would deter offenders, and thus, prevent the crime from taking place. While findings are mixed, some perceptual deterrence research shows that offender decision making can be influenced by these crime prevention tactics (e.g. Decker et al. 1993). Since cyber-trespassing is often a pre-cursor crime to cyber-theft, it follows that if cyber criminals were dissuaded from trespassing, then cyber-theft should also decrease as well. Notably, since non-technical methods can be used to obtain the personal information used in cyber-theft, it is plausible that elimination of cyber-trespass will not fully eliminate cyber-theft. Tactical displacement may occur.

Clarke (2010) proposes that there are five aspects related to decision-making, that if modified, can prevent crime by influencing the offender's assessment of crime opportunity—(1) increasing the effort required to commit the crime, (2) increasing the risks of detection and apprehension, (3) reducing the rewards that may accrue from the crime, (4) removing the provocations that may trigger offending behavior, and finally, (5) removing the excuses that may be used by offenders to justify their actions. Within each category, there are specific opportunity reducing techniques, resulting in a total of 25 opportunity reducing techniques that can be applied to dissuade potential offenders from choosing and acting against targets (see Table 1).

Table 1. Situational Crime Prevention Table Applied to Cyber security

Increase the Effort	Increase the Risks	Reduce the Rewards	Reduce Provocation	Remove Excuses
1. *Target hardening*, e.g., Anti-virus software, installing a firewall, and physical lock for PC	6. *Extend guardianship*, e.g., monitor PC functions	11. *Conceal targets*, e.g., hide Wi-Fi network, conceal PC name on public networks, minimize ID of offices	16. *Reduce frustrations and stress*, e.g., host hacking challenges with prizes	21. *Set rules*, e.g., use more disclaimers on forums about hacking computers that an individual owns and information security policies
2. *Control access to facilities*, e.g., use a password on crucial computer functions, restrict who uses the computer, and biometric fingerprint authentication	7. *Assist natural surveillance*, e.g., open plan offices	12. *Remove targets*, e.g., do not store personal data on PC, isolate sensitive information from network, and clear desks and computer screens	17. *Avoid disputes*, e.g., do not post inflammatory statements	22. *Post instructions*, e.g., post security protocol at work stations
3. *Screen exits*, e.g., use reception desks and system time outs	8. *Reduce anonymity*, i.e., link forum users to a verified Facebook account	13. *Identify property*, e.g., monitor dark web for personnel identifiers and mark property	18. *Reduce emotional arousal*, e.g., do not promote hacking videos or posts	23. *Alert conscience*, e.g., have pictures of family on PC, formal reminders of acceptable usage, and warning messages when logging in
4. *Deflect offenders*, e.g., disconnect important computers from the internet, off-site storage of data, use honeypots, and segregation of duties and program access	9. *Utilize place managers*, e.g., automatic firewall monitoring, check on PC for weird behavior, and audit computer logs	14. *Disrupt Markets*, e.g., Take down dark web markets	19. *Neutralize peer pressure*, e.g., do not encourage people to hack	24. *Assist compliance*, e.g., set up fake websites for other hackers to try their skills on and security education for staff
5. *Control tools/weapons*, e.g., monitor who has access to botnets and immediately delete access of ex-employees	10. *Strengthen formal surveillance, e.g.,* install an intrusion detection system and two-person sign-off on new accounts	15. *Deny benefits*, e.g., encryption on data files in computer and alarms on laptops	20. *Discourage imitation*, e.g., update computer software after the fact.	25. *Control drugs and alcohol*, e.g., do not use the computer when drunk

Several studies investigated the utility of the SCP framework and the effectiveness of specific techniques in reducing crime. 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, and retail 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 initiatives, broadening SCP's application to include social crimes. More germane to the present study, two prior studies used SCP to think about how to defend computer systems.

Willison and Siponen (2009) contend that practitioners would benefit from using crime scripts to investigate specific types of insider computer crime when using SCP to develop security protocol. Crime scripting involves dissecting specific crimes into the steps needed to complete the act. Using computer fraud as an example, they argue that each computer crime can be dissected into a universal set of 9 functions—preparation (e.g., gaining access to the organization), entry (e.g., authorized employee), pre-condition (e.g., wait for employee to leave), instrumental pre-condition (e.g., access someone else's computer), instrumental initiation (e.g., access programs), instrumental actualization (e.g. create a false customer account), doing (e.g. create fake invoices), post condition (e.g. close programs), and exit (e.g. leave facility). Then, security specialists can apply the 25 techniques to computer systems to develop a full set of opportunity reduction techniques for each step/function. While these authors present a powerful argument, they did not follow-up by demonstrating the utility of a script-SCP approach with a sample of practitioners.

Research by Hinduja and Kooi (2013) also reason that applying SCP would benefit the information security sector. They go on to state, however, that not all aspects of SCP could be applied—only 16 of the 25 techniques were relevant to information security in a cyber-setting. These researchers also state that there were two main limitations to how SCP can be applied to a cyber-based information system. The first is that there was cause for concern for adding more surveillance to the online ecosystem—such measures may not be politically palatable. Second, they state that it takes time for security measures to be implemented making it difficult to implement when the field of information security changes rapidly.

Combining the examples provided by Willison and Siponen (2009), and Hinduja and Kooi (2013), Table 1 demonstrates that when information security is considered broadly it is feasible to find examples for each SCP technique. Whether the SCP framework is useful for *specific* cyber-crimes is yet to be determined. To date there have been no attempts to empirically test the utility of SCP for classifying strategies to prevent the related crimes of cyber-theft and cyber-trespass.

2. Offenders' use of Situation Crime Prevention

Offenders are often overlooked when it comes to research about victimization. And yet, criminals are just as susceptible to crime as non-criminals, as such, there is much we can learn about the effectiveness of crime prevent from this population (e.g., Cromwell & Nielson 1999). Addressing this gap in the literature, studies are beginning to document offenders' use of crime prevention techniques. Drug dealers are the most studied offender type. For example, investigating whether offenders use situational prevention techniques to defend themselves from victimization, Jacques and Reynald (2012) conducted interviews with 50 drug dealers. Offenders employed all categories of SCP in some form to protect themselves. In another study, Jacques, Allen, and Wright (2014) looked at the choices that drug dealers make when they defrauded by buyers. While not investigating SCP directly, interviews with drug dealers revealed that not using place managers or failing to reduce exposure increased the likelihood of being ripped-off. From interviews and observation of a sample of 33 drug dealers, Dickinson and Wright (2015) found that gossip spread from other dealers was used to spot troublesome individuals and make decisions to avoid problems. Investigating the defensive techniques of open-air drug dealers selling on the street in New Jersey, Piza and Sytsma's (2016) used the Newark Police Department's security cameras to observe 92 separate drug transactions. The researchers found that drug dealers used many situational prevention techniques, i.e., drug dealers kept stashes on their person to prevent theft of drugs.

In the digital age it is increasingly important to investigate cyber offender victimization, and defensive behavior. As noted above, offenders routinely employ techniques to protect themselves from law enforcement, other criminals, or from upset customers (e.g., Jacques & Reynald, 2012; Piza & Sytsma, 2016). Cyber criminals often use the same technology as non-cyber criminals; therefore, their computers and habits may contain the same vulnerabilities that allow make them susceptible to victimization. And, even though some people have more technical skill and knowledge about security, as a group, this population are likely to spend a lot of time online, and more exposure suggests a greater potential for victimization (Pratt, Holtfreter, & Reisig, 2010).

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. Individuals involved in cybercrime are apt to develop significant subject matter expertise. Since cyber criminals exploit the effectiveness of security measures, their knowledge and experience with cyber-theft provides insight into internet enabled crime. In other words, understanding cyber vulnerabilities from the offenders' perspective is crucial because these are the people who commit the crimes, therefore, the methods they employ to protect themselves should be the most effective measures. Accomplishing that, one could use these strategies to develop a set of *routine precautions* to help people to avoid victimization online (Felson & Clarke, 2010).

Methods

1. Data Source

To investigate which counter measures are recommended to prevent against cyber-trespass and theft, data were collected through a content analysis of websites that have some connection to the hacking community. Online forums were selected because prior research shows that informal communication like gossip enables offenders to identify threats and take action to avoid victimization (e.g., Dickinson & Wright, 2015). We reasoned that among members of an online hacker community, information dissemination may spread in a gossip-like manner through message boards. To avoid an ethical dilemma, we decided against direct communications with self-identified hackers, choosing instead to draw on publicly accessible communications. We decided that gaining trust online might require posing as a novice hacker and this would constitute a violation of the standards of research ethics for human subjects.

Not all public forums about hacking are produced by the hacking community. For this reason, we developed specific research protocol to uncover websites that purport to offer hacking news or strategies. Websites were identified using a basic google search using the terms "hacking", "hacking community", "hacking forums", and "hacking sites". The term hacking was used as the academic labels of cyber-trespass and theft are not commonly used by the target population in these venues. Hyperlinks were examined and all qualifying sources were included in the study. Eligibility criteria included four conditions: (1) the site focused on hacking behavior; (2) material was posted in English; (3) the site was accessible through Google (no dark web sites were used); and, (4) the site or material was not paid advertisement for a product. In total, 134 websites were identified, and from those websites, 24 contained information about crime prevention strategies (see Appendix A for a list of websites).

Six of the 24 sites were forums or fan pages and 18 were static posts or blogs (75% of sites examined were static posts or blogs). *Forums* are websites that contain message boards for a subject where users make posts that other users can respond to. There were two general types of forums: (1) forums that typically cover only one subject, that are maintained by individuals who pay for a server to host their website; and (2) forums hosted by third parties that permit users to freely create fan pages, where users can post topics of conversations for others to post replies without having any advanced coding skills (e.g., Reddit). *Static posts* are blogs or websites 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.

To find relevant content, each of the 24 websites were searched with the terms "security", "protection", "safety", "protect", "protect yourself", "protection tips" and "safety tips". Sample identification lasted from 12/21/2017 to 01/16/2018. Original posts and user replies were included in this study. In total, 85 web pages contained tips and strategies to prevent online victimization. Table 2 reports how many websites were uncovered from forums and blogs.

2. 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). Using a top-down coding process, each strategy named in a webpage as a technique that could be deployed by an individual to prevent victimization was captured as a node. Each node was labeled with one of the 25 opportunity reducing techniques of SCP. Where strategies could fall under two opportunity reducing classification, the best fitting technique was selected. Nodes received only one classification. The full list of 25 opportunity reducing techniques of SCP, complete with examples of cyber SCP for each technique (Willson & Sipinen, 2009), was on hand to ensure reliable coding.

In addition, each strategy was rated as either *expert*, meaning that the advice was intended for users with extensive computer knowledge, or *novice*, which was advice where little to no computer knowledge was needed to deploy the protective measure. More specifically, the protective measure was considered expert if it involved coding or other actions that could not be set in a program's settings; protective measures were coded as novice if a user could enact the suggestion with little to no effort, e.g., clearing search history.

Coding uncovered 379 references to specific protective measures. Some measures were mentioned several times. Sample characteristics are reported in Table 2.

Table 2. Sample Description, n=85 pages

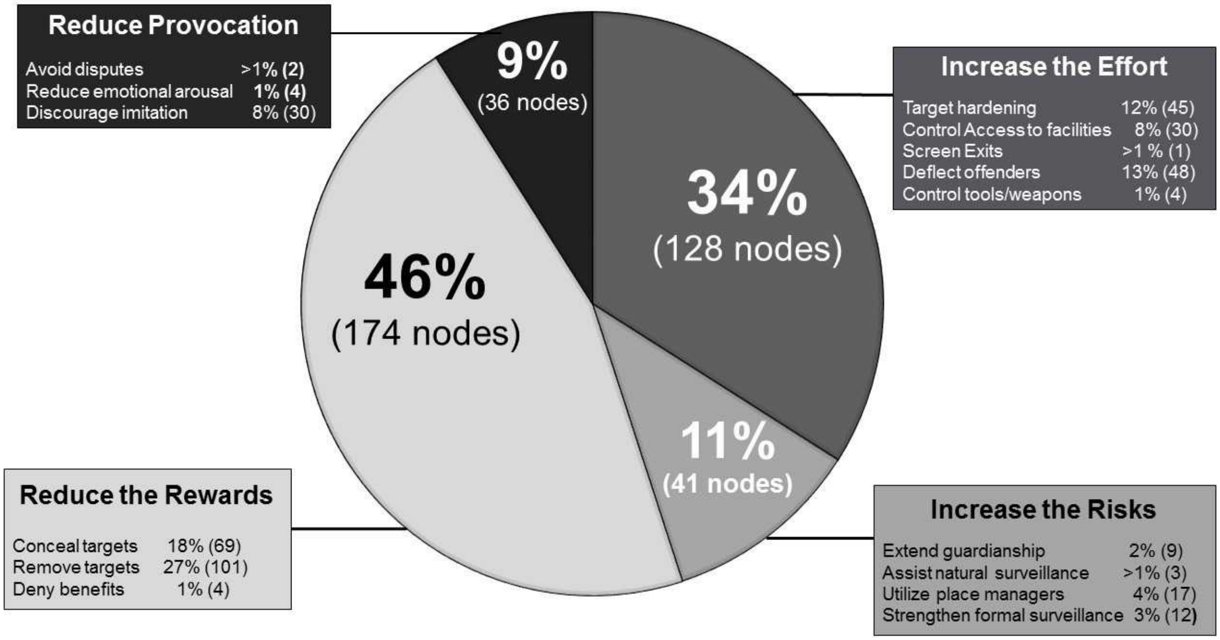
Variable	N	%
Sources		
Individual Forums	20	24%
Third Party Forums	17	20%
Static Posts/Blogs	48	56%
SCP Technique Category		
Increase the effort	58	68%
Increase the risks	31	36%
Reduce the rewards	57	67%
Reduce provocation	26	31%
Remove excuses	0	0%

Results

1. Prevalence of Opportunity Reducing Techniques

Overall, the full SCP framework was not represented in the security advice examined. No protective strategies were categorized as efforts to remove excuses; as such, it does not appear in Figure 1. The figure reports how common opportunity reducing techniques were relative to each other (N=379 nodes; where a node is a piece of advice).The two most prevalent categories were increase the effort and reduce the rewards, 34% and 46% respectively.

Figure 1. Distribution of Recommended Prevention Strategies



Note: Percentages are based on the grand total.

a. Increase Effort

Within the category, increase effort, the most common technique mentioned was deflecting offenders (13% of nodes). 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”; and, “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 we found that using a strong password was the most common (9 instances). Next in popularity, were recommendations to use safer software such as Firefox or Linux (6 instances) and to change passwords often (6 instances). Five recommendations suggested using software to block automated processes on websites such as pop-ups and scripts, and three nodes advised to use sandbox software to open suspicious files.

Two other SCP 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 nodes, the most frequently mentioned tactic was installing anti-virus or anti-malware programs (22 instances), e.g., "*Install Adware"; "Install a good Antivirus/Anti-spyware"; and, "Spend a few bucks on a good anti-spyware program.*" Not as common, but worth mentioning, were the 30 instances of advice recommending counter measures classified as actions to control access to facilities (8% of nodes). The two most noteworthy recommended strategies were to use a firewall (8 instances) and use a password (5 instances). Examples of other advice in this category include: "*restricted connectivity"; "enabling HTTPS for all logins and wp-admin"; and, "Restrict direct access to plugin and theme PHP files.*"

The remaining five suggestions were classified as actions that would control tools (1%) or screen exits (.2%). Examples follow:

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

b. Increase the Risks

While counter measures aimed at increasing offending risks were less prominent (11% of nodes), suggestions to use place managers were most common (4% of nodes)—that is, use third-party websites to examine web traffic with (6 instances) and to look for flaws inside of a server (3 instances), and to use Virus Total to scan files before opening them (2 instances). Some other recommendations include: *"Download from known sites"* because they are likely to monitor their content and *"Use two factor authentication as much as possible."*

About 3% of nodes were suggestions to strengthen formal surveillance. Within this category, the most frequently recommended strategy was to run some sort of scan on your important files (8 nodes). Suggestions include: *"Scan your PC once a week"; "don't want to limit yourself to one antivirus program"; and "Perform an endemic test at the documents/e-mail attachments which you down load before executing them."*

Taking actions to extend guardianship was suggested infrequently (2% of nodes). Of note, hackers suggested to regularly check any activity on important data—"*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";* and, *"Always Check the URL in the Address Bar"*

Finally, less than 1% of the nodes referred to protective measures that would assist natural surveillance. Examples 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"*, and *"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"*

c. Reducing Rewards

Protective measures recommended most often on forums associated with the hacking community were classified as measures that would reduce the rewards associated with cyber-trespass or theft; a total of 46% of nodes involved actions meant to reduce rewards. Within this category, actions designed to remove targets were advised most often (27% of nodes). Within this SCP technique, not clicking on suspicious links was frequently recommended (11 times), as was suggestions to refrain from using public computers / Wi-Fi (10 times), or downloading or clicking on suspicious email (7 times). Also, people were advised to avoid installing plug-ins and toolbars onto their browsers (5 instances). Some other examples of removing targets are: *"Do not click on popups"; and "NEVER double-click the pen drive to open it. Instead right-click on it and select the option 'open'."*

About 18% of nodes advised people to enact strategies that would conceal targets. Within this category, the strategy most recommended was use a VPN when browsing the internet (23 instances). After that, the next most frequently recommended protective measures were to encrypt data (13 instances), use a Virtual Machine on your computer (7 instances), use an anonymous browser like Tor (5 instances), and use a password management software (5 instances). Some other suggestions include: "*disable the on- screen SMS previews*"; "*Encrypt Your Wireless Router Connection*"; and, "*Never Put Author Usernames on Display."*

Finally, 1% of the total coding involved strategies that would act to deny the benefits associated with cyber-trespass or theft. Examples of this SCP technique include: "*keeping around a known-good firmware image and wiping your hard drive + reflashing the firmware every month*" and "*use Android Device Manager.*"

d. Reduce Provocation

About 9% of the nodes referred to protective actions best classified as measures that reduce provocation. Within this category, measures to discourage imitation figured prominently (8% of the sample). There were 30 instances of recommendations to keep your software and devices updated. This was classified as reduce provocations because it is a known exploit that hackers might look for first when deciding which computer to hack. Recommendations include: *"It is highly recommended that you turn on the automatic update feature"; "Install Updates Frequently";* and, *"Patch everything, immediately"*. Less than 2% of nodes advised to reduce emotional arousal (e.g., *"Revert the SSO system back to OAuth 2";* and, *"Change your default passwords"* or avoid disputes (e.g., "*Don't try to hack others").* (These measures were classed as removing the temptation of an easy target, recommendations to install a specific system would change the classification to target hardening.)

2. Level of Expertise

One of the questions driving this study was whether the advice recommended by self-identified members of the hacker community was geared towards novices or experts. We were curious to know what level of technical skill was required to implement the recommended security precautions. Interestingly, we found that most of techniques being recommended could be implemented by novices with little computer knowledge—novice protective measures comprised 90% of the total nodes.

Novice-level advice included:

- *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*

To illustrate the difference, expert-level skills are required to implement the following suggestions.

- *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*

Discussion

The general aim of this study was to investigate whether the counter measures for cyber-trespass and theft that are being discussed within the hacker community fit within the framework of SCP. Underlying the aim of the study was a desire to investigate the efficacy of the framework for specific cyber-crimes and to explore the utility of using potential offenders as advisors when developing recommendations on routine precautions that people could use to protect themselves online. We reasoned that individuals who post advice on hacker forums are knowledgeable about the risks and vulnerabilities inherent to online activity. Extrapolating on arguments made by Jacques and Reynald (2012) and Pratt et al. (2010), we assert that understanding cyber-trespass and theft vulnerabilities from the perspective of the hacker community is crucial because these individuals may have insider information. It follows that the methods they employ to protect themselves from cyber-trespass and theft should be the most effective measures. And once identified, these strategies could be bundled to develop a set of routine precautions to help people to avoid victimization online (Felson & Clarke, 2010).

1. Utility of the SCP Framework

We discovered that even though the SCP framework was not fully realized when applied to cyber-theft, and the related pre-cursor crime of cyber-trespass, it is useful for thinking about cyber-crime. Our findings are comparable to other studies: prior studies encountered similar challenges to applying SCP to classify cyber protective measures. For example, Willison and Siponen (2009), tried to apply the 25 techniques of SCP to information security more generally. While they were able to produce a modified SCP table with several examples, they failed to identify examples of all of the SCP techniques. Willison and Siponen concluded that the result may be a function of industry efforts and that empty cells identified areas to be looked at further by practitioners (2009). Hinduja and Kooi (2013) applied 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 more recent expanded list of techniques.

Echoing Hinduja and Kooi (2013), we assert that the protection measures recommended within the hacker community fit parts of the SCP framework well. Reduce the rewards was the largest category, and, the most recommended technique within this category was to engage in actions that would remove targets. Investigating the nature of the recommended protective measures more closely, we discovered that among the online community of self-appointed hacking experts, advice to protect against cyber-trespass and theft online did not commonly involve high-tech strategies, rather most suggestions could be implemented by novices. For example, not clicking on suspicious links, not downloading suspicious files, and avoiding suspicious emails. This advice is consistent with research that attacks are more often perpetrated by opportunistic hackers using simple strategies, i.e., waiting for people to click on links (Madarie, 2017; Thycotic, 2014, 2017).

Noting that other studies applying the SCP framework to offenders' protective actions uncovered strategies for all of the main categories of SCP (e.g. Jacques & Reynald, 2012), we acknowledge the wisdom contained in the arguments made by Willison and Siponen (2009). Just because we did not find prevention measures that could be classified as techniques aimed at removing the excuses for crime, it does not mean that the category is inapplicable. Rather, the hacking community, as represented by the pages examined, offers advice to protect against victimization, it does not aim to dissuade people from hacking. It would be counter-normative for the hacking community to remove excuses for cyber-trespass (though an argument could be made that some faction of the community might be against cyber-theft.)

Additionally, even within the most represented category of SCP techniques, reducing the rewards associated with crime, some specific techniques were not represented, i.e., measures to identify property and disrupt markets were not mentioned in the sources consulted. Again, deploying such measures may be counter-normative. Of concern, our findings draw attention to the limitations of using potential offenders as sources of crime prevention expertise. Relying solely on offending populations for information on the effectiveness of crime prevention strategies raises a validity threat. In addition to inherent normative biases, the offending community is not omnipresent and there are limitations to their experience. For these reasons, triangulating between information sources is necessary to address the inherent biases associated with each field of expertise so as to develop a more complete package of interventions.

2. Implications for Protecting against Cyber-Trespass and Theft

Given the low-technology, novice-level nature of most protective measures recommended by the sample of advice examined, it is feasible that a package of interventions could be implemented as a set of routine precautions. *Routine precautions* are defined as the naturally occurring steps we take to protect ourselves such as locking our doors and avoiding going out at night (Felson & Clarke, 2010)

To develop a set of routine precautions, Felson and Clarke argue that we must first identify specific situations that allow offenders to commit those crimes (2010). What then, are the situations where cyber-trespass and theft takes place? While this study did not investigate the context of victimization, inferences can be drawn from the recommendations. For instance, the most recommended strategies were to keep your software updated and to use device and software security settings such as, strong passwords that are changed often. This suggests that cyber-trespass is more likely to occur through efforts to break through outdated software via lax security. Other advice frequently given include simple strategies such as: do not click on suspicious links; only download from trusted websites and sources; run a virus scan before executing any downloaded programs; do not rely on a single antivirus or anti-spyware program, use several good ones; block automated process like pop-ups; use "safer software" like Firefox or Linux; and use a sandbox program to open suspicious files. These protective measures address actions related to surfing the web and obtaining and opening files (and programs).

Other less commonly suggested measures were clearly directed toward individuals with deeper computing knowledge who engage in more advanced computer work, e.g., use two factor authentication; use 3rd party websites to examine web traffic and look for flaws inside servers; invoke endemic tests of documents and attachments; restrict direct access to wp-admin directory, plugins and theme PHP files; resolve the subdomain takeover of saostatic.uber.com by removing the dangling CNAME to AWS CloudFront CDN; and, make a // entry in config.php that displays the WordPress table prefix used in the installation. The situational context inferred by these suggestions pertains to a higher level of routine computer work and online foraging that exceeds what the general public is likely to engage in.

The next question to ask is, what should be done to adopt routine precautions against cyber-trespass and theft? Felson and Clarke conclude that governments will need to become involved and will increasingly rely on routine precautions to prevent crime (2010). They state that there are multiple factors to consider—the range and prevalence of routine precautions, the availability of public and private resources, inconvenience and opportunity costs, effectiveness and efficiency as crime prevention measures, and other benefits from feeling empowered to control the problem. Once governments are onboard with promoting routine precautions, then the challenge becomes getting citizens to adopt these actions. Felson and Clark suggest 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.

When applied to internet crimes these methods might involve:

- Formal social controls – mandating higher traffic or system critical websites and software to force users to change their passwords to thwart people from compromising those passwords.
- Informal supervision–encouraging the public to avoid suspicious links and to update their computer software.
- Signage and instructions–requiring email services displaying messages not to download attachments from unknown senders.
- Products designed to facilitate routine precautions – requiring computers to automatically update their software.
- Designs that improve natural surveillance–requiring a computer or a website that hosts files to install an anti-virus software to scan files before they are made public.

Felson and Clarke (2010) recommend that routine precautions be 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 combating 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 individuals that were self-identified to be part of the hacking community. Furthermore, Thycotic (2014) found that 88% of hackers surveyed believe their information is at risk. This high level of perceived risk might partially explain why we found 24 unique websites and 85 associated pages dedicated to sharing protective advice. Therefore, these precautions should be considered as routine precautions. As Jacques and Reynald (2012) stated there is a need to learn from offenders to protect ourselves. While there is no way to confirm that the individuals posting advice on the web pages examined were experienced hackers, given the nature of the websites they chose we have reason to suspect that they are self-identifying as being part of the hacking community.

Conclusion

Cyber theft is a costly crime, impacting those who are most vulnerable (ICCC, 2016; McAfee, 2018).Quelling the coming wave of cybercrime might necessitate exploration of new avenues of research such as examining offenders' perspectives. With this goal in mind this paper sought to find out how the hacker community defends itself. Using the SCP framework, we found that removing targets was the most common technique with 27% of advisements. Results also showed that 90% of all advice given could be used by those with little computer knowledge. Finally, consistent with prior research (e.g., Hinduja & Kooi, 2013), we found that SCP had limitations on how it could be applied to stop cyber theft and trespass, in part because this class of crime does not always require direct victim-offender interaction.

With these results in mind, routine precautions might be the key to preventing cyber theft and trespass. Cyber-oriented suppliers should be required to build more simple routine precautions into their products. This research found that self-professed members of the hacking community are not overly concerned with professional, highly-skilled attacks, rather their advice would thwart recreational opportunists. This study demonstrates that much can be learned that will advance cybercrime prevention from listening to potential offenders themselves.

Limitations

This study is not without its limitations. Most importantly, the strategies recommended were classified under a specific technique using a best fit protocol. Consequently, 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, best judgement was used to classify it as one technique. This classification protocol may have introduced a reproducibility threat: some protective measures could be placed into other techniques if coded in a different study. Additionally, while these strategies were recommended by self-professed members of the hacking community, there was no data to suggest how effective each strategy was in preventing crime and we do not know for certain if the individual sharing advice was an experienced hacker. Also, we 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 publicly accessible website included was Reddit—the lack of darknet and private discussion forums may have influenced our findings. Due to these limitations, it would be premature to use our finding to make theoretical implications for the enhancement or modification for the SCP framework.

References

Anderson D., Chenery S. & Pease, K. (1994). *Preventing Repeat Burglary and Car Crime*. Crime Detection and Prevention Paper 58, London: Home Office

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

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

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.

Cromwell, P., & Nielsen, A. L. (1999). *In Their Own Words: Criminals on Crime*. Los Angeles, CA: Roxbury Publishing.

Decker, S., Wright, R., &Logie, R. (1993). Perceptual Deterrence Among Active Residential Burglars: A Research Note. *Criminology, 31*(1), 135-147.

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.

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.

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.

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

*I*C3 (2016). *Internet crime report*. Washington, D.C.: National White Collar Crime Center.

Jacques, A., & 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. (2012). The Offenders' Perspective on Prevention. *Journal of Research in Crime and Delinquency, 49*(2), 269-294. doi: 10.1177/0022427811408433

Jaishankar, K. (2018). Cyber Criminology as an Academic Discipline: History, Contribution and Impact. *International Journal of Cyber Criminology*, *12*(1), 1-8.

Jaishankar, K. (2009). The Future of Cyber Criminology: Challenges and Opportunities. *International Journal of Cyber Criminology*, *4*(1&2), 26-31.

Kshetri, N. (2016). Cybercrime and Cybersecurity in India: Causes, Consequences and Implications for the Future. *Crime, Law and Social Change, 66*(3), 313-338.

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

McAfee. (2018). *Economic Impact of Cybercrime – No Slowing Down*. Washington, D.C.: James Lewis

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.

Ngo F., & Jaishankar K. (2017). Special Article: Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime. *International Journal of Cyber Criminology*, 11(1), 1-9.

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

Thycotic. (2014). *Black Hat 2014 Hacker Survey Executive Report*. Washington, DC

Thycotic. (2017). *Black Hat 2017 Hacker Survey Report*. Washington, DC.

Wall, D. S. (2001). Cybercrimes and the Internet. In D. S. Wall (Ed.), *Crime and the Internet* (pp. 1–17. New York: Routledge.

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