Routledge
Taylor & Francis Group

Victims & Offenders

An International Journal of Evidence-based Research, Policy, and Practice

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uvao20

Phishing Evolves: Analyzing the Enduring Cybercrime

Adam Kavon Ghazi-Tehrani & Henry N. Pontell

To cite this article: Adam Kavon Ghazi-Tehrani & Henry N. Pontell (2021) Phishing Evolves: Analyzing the Enduring Cybercrime, Victims & Offenders, 16:3, 316-342, DOI: 10.1080/15564886.2020.1829224

To link to this article: https://doi.org/10.1080/15564886.2020.1829224

Published online: 16 Feb 2021.

VICTIMS & OFFENDERS
2021, VOL. 16, NO. 3, 316–342
https://doi.org/10.1080/15564886.2020.1829224

Routledge
Taylor & Francis Group

Phishing Evolves: Analyzing the Enduring Cybercrime

Adam Kavon Ghazi-Tehrani [a] and Henry N. Pontell [b]

[a]Department of Criminology and Criminal Justice, University of Alabama, Tuscaloosa, Alabama, USA;
[b]Department of Sociology, John Jay College of Criminal Justice, New York, New York, USA

ABSTRACT

Phishing, the fraudulent attempt to obtain sensitive information by disguising oneself as a trustworthy entity via electronic communication, has quickly evolved beyond low-skill schemes that relied on casting "a wide net." Spear phishing attacks target a particular high-value individual utilizing sophisticated techniques. This study aims to describe the current state of phishing, the expected technological advances and developments of the near future, and the best prevention and enforcement strategies. Data comes from interviews with approximately 60 information technology security professionals, "hackers," and academic researchers. Routine Activity Theory provided an operational framework; while it is an imperfect fit for most crimes, it provides enough explanatory power for cyber-crimes. Interviewees mainly agreed: First, technological advances increase the proliferation of phishing attacks, but also aid in their detection. It has never been easier to conduct a simple attack, but a good attack requires more effort than ever before. Second, phishing is directly responsible financial fraud and, indirectly, as the primary attack vector for ransomware. Third, newer types of attacks utilizing technology, like deepfakes, will make the problem worse in the short-term. Fourth, prevention will come from machine learning and public education akin to WIFI security improvement via the combination of encryption and password awareness.

KEYWORDS

victimization; theories; routine activities; Technology

Introduction

Phishing is an automated form of social engineering whereby criminals use the Internet to fraudulently extract sensitive information from businesses and individuals, often by impersonating legitimate web sites. The high potential for rewards (e.g., through access to bank accounts and credit card numbers), the ease of sending forged e-mail messages impersonating legitimate authorities, and the difficulty law enforcement has in pursuing the criminals responsible have resulted in a surge of phishing attacks in recent years (Egan, 2020). The 2019 "State of the Phish" report found that nearly 90% of organizations experienced targeted phishing attacks in 2019, 84% reported SMS/text phishing (smishing), 83% faced voice phishing (vishing), and the volume of reported e-mail increased 67% year over the previous year (Egan, 2020). Evidence suggests that an increasing number of people shy away from Internet commerce due to the threat of identity fraud, despite the tendency of companies to assume the risk for fraud (Morrison & Firmstone, 2000).

CONTACT Adam Kavon Ghazi-Tehrani akghazitehrani@ua.edu Department of Criminology and Criminal Justice, University of Alabama, Tuscaloosa, AL 35487-0320, USA.

A typical phishing attack begins with an e-mail to the victim, supposedly from a reputable institution, yet actually from the *phisher*. The text of the message commonly warns the user that a problem must be immediately corrected with the user's account. The victim is then led to a *spoofed* website (a fake one designed to resemble the institution's official website) (Alsharnouby et al., 2015). In this passive attack, the web page prompts the victim to enter account information (e.g., username and password) and may also request other personal details, such as the victim's Social Security number, bank account numbers, ATM PINs, etc. All of this information is relayed to the phisher, who can then use it to access the user's accounts (Alsharnouby et al., 2015).

Phishing has remained a costly cybercrime for businesses and individuals. It is directly responsible for financial loss due to fraud, and causes damage indirectly as the primary attack vector for ransomware, where the victim's computer files are locked by intruders until payment is made to them (Gorham, 2020). From 2013–2018 the FBI found that Business E-mail Compromise (BEC) accounted for 12 USD billion in direct losses to US corporations and that ransomware attacks cost corporations 7.5 USD billion in 2019 alone (O'Neill, 2020).

Past studies (Hutchings & Hayes, 2009; Kigerl, 2012; Reyns et al., 2011) have analyzed *phishing* within the Routine Activity theoretical framework. Though various criminological theories have been utilized to explain cyber-crime, including social learning theory, self-control theory, and subcultural theories (Stalans & Donner, 2018), these remain offender-focused methods of explanation. To analyze why *phishing* exists, persists, and what may be done to combat it, situation-focused theory is more appropriate (Wortley & Tilley, 2014). Routine activity (Cohen & Felson, 1979) is a situational theory of crime opportunity that provides a tool for analyzing the efficacy of both technology-focused (*target hardening*) and human-focused (*capable guardians*) efforts to combat *phishing*. This allows policy suggestions that aim to reduce risk of victimization to be tested (Leukfeldt, 2014, 2015; Leukfeldt & Yar, 2016).

This study seeks to define the factors that lead to *phishing* enduring as a crime type and to refine the application of Routine Activity Theory to cyber-crimes. It also aims to describe the current state of phishing, the expected technological advances and developments in the near future, and the current state of prevention and enforcement strategies in order to further improve them.

The paper is presented as follows. First, a literature review summarizes the extent of phishing scholarship and identifies gaps in current research regarding phishing. Second, the methodology for the study is described, including the research plan, data collection and coding issues, research questions and planned analysis. Third, the data are analyzed and findings are presented through a series of "relevant, emergent codes," which allow for the labeling of concepts that become apparent during data collection and analysis. Finally, there is a discussion of the findings regarding phishing in both the present and future, potential control mechanisms, and an assessment of the utility of applying Routine Activity Theory to cyber-crimes in general. Limitations of the study and suggestions for future research are offered, as well as policy implications.

Literature review

Routine Activity Theory

There remains debate within cyber criminology about the similarity of cyber-crimes to terrestrial ones and the viability of using "traditional" criminological theory to analyze digital crimes (Grabosky, 2001). Cohen and Felson's (1979) Routine Activity Theory (RAT), created to explain crime patterns in post-WWII Chicago, is the most frequently applied criminological theory for understanding cyber-crime victimology (Bossler & Holt, 2009; Hutchings & Hayes, 2009; Leukfeldt, 2014, 2015; Leukfeldt et al., 2016; Leukfeldt & Yar, 2016; Ngo & Paternoster, 2011; Pratt et al., 2010; Reyns et al., 2011; Van Wilsem, 2011, 2013). The routine activity approach holds that victimization is influenced by a combination of a *motivated offender*, a *suitable target*, and an *absence of a capable guardian* in a convergence of time and space (Cohen & Felson, 1979). The *motivated offender* is an assumed property, *tuitable targets* are determined by VIVA: Value, Inertia, Visibility, and Access, and *capable guardians* may be people, such as police, or things, such as security cameras (Cohen & Felson, 1979).

Routine Activity Theory has also been advanced since its original conception by Clarke et al. (1999), who extended Cohen and Felson's (1979) work on target suitability to explain the phenomenon of "hot products, " or those that can be stolen easily and that share six key attributes of being CRAVED; they are concealable, removable, available, valuable, enjoyable and disposable (Clarke et al., 1999). Their research suggests that relatively few hot products account for a large proportion of all thefts (Clarke et al., 1999).

The theory is not perfectly adapted for virtual settings, however, and Yar (2005) argues that it is problematic to convert the routine activity approach from real space to cyber space, due to issues of spatiality, temporality, and the tenuous comparison of physical guardians to virtual ones. The critiques presented by Yar (2005) are definitional, rather than practical. For example, Yar (2005) argues that Routine Activity Theory requires both a rhythm, or "regular periodicity with which events occur," and a timing, in which different activities are coordinated "such as the coordination of an offender's rhythms with those of a victim" (Cohen & Felson, 1979, p. 590). *Phishing* is usually an asynchronous act: a compromised e-mail is sent to the intended victim and the victim opens it at some later time. In this case, using a narrow interpretation of Routine Activity Theory, a temporal convergence will not occur. Instead, a wider interpretation allows for the temporal convergence to be between the victim and the *phishing* e-mail, rather than the victim and the offender.

Though every facet of Routine Activity Theory may not map perfectly from real space to virtual space, numerous studies have supported its application for cyber-crimes, generally, and *phishing*, specifically. Hutchings and Hayes (2009) found that users who spend more time online are more likely to be *phished* by increasing their "exposure" as a *suitable target* to possible offenders and that users who do not utilize spam filters (*capable guardians*) are also more likely to fall victim. Bossler and Holt (2009) found similar results when analyzing other types of cyber victimization within a population of colleges students. In their study, Bossler and Holt (2009) discovered that while respondents' general computer use and activities such as playing video games, shopping, or checking e-mail did not have a significant impact on the likelihood of experiencing online victimization, the number of hours respondents spent in chat rooms and using instant message (IM) chat did.

Also, Leukfeldt and Yar (2016) later show that the explanatory power of Routine Activity Theory differs greatly between different types of cyber-crime, but that factors which matter for *phishing*, such as target *value* and *visibility* were significant in predicting victimization. *Phishing* is one type of cyber-crime that seems particularly well-suited to the theory. While the temporal and physical elements are removed via online contact, the combination of a *suitable target* (sensitive information) and the absence of *capable guardian* (an uninformed end-user) would appear to result in a higher likelihood of phishing victimization.

Types of phishing

The vast majority (96%) of phishing attempts are made via e-mail (Verizon, 2019). In the past, these e-mails were poorly-worded, low-effort attempts sent to a large number of people (for example, in batches of hundreds of thousands) with the expectation that even a low response rate (~0.5%) would still yield hundreds of victims (Egan, 2020). Widespread use of "spam" filters, however, has made this brute-force methodology increasingly ineffective and *phishers* have turned to more advanced techniques (Cook et al., 2009). These include: Business E-Mail Compromise (BEC), Smishing, Vishing, Spear phishing, and Whaling (Parmar, 2012).

BEC occurs when a cybercriminal sends an e-mail to a lower-level employee, typically someone who works in the accounting or finance department, while pretending to be the company's CEO or another executive, manager, or supervisor (Mansfield-Devine, 2016b). The goal of these e-mails is often to get their victim to transfer funds to a fake account while preying on the tendency for most employees to not question their workplace superiors (Mansfield-Devine, 2016b).

Smishing is short for "SMS phishing;" SMS is "short message service," the standard the world uses for text messaging (Stembert et al., 2015). Smishing attacks utilize phone text messages as the attack vector, instead of e-mails, partially to bypass SPAM filters and to reach more potential victims. *Vishing*, short for "voice phishing" uses telephone calls to accomplish the same, for similar reasons (Stembert et al., 2015).

Spear phishing has risen in popularity as earlier "simple" mass phishing has declined; a *spear phishing* attack is targeted (Parmar, 2012). Unlike general phishing e-mails, which use spam-like tactics to reach the general population in massive e-mail campaigns, spear phishing e-mails target specific individuals within an organization employing various social engineering tactics to tailor and personalize the e-mails to their intended victims. For example, they may use subject lines that would be topics of interest to the recipients to trick them into opening the message and clicking on links or attachments. *Whaling* is a form of *spear phishing* and can be viewed as the "opposite" of BEC (Stembert et al., 2015): Instead of targeting lower-level individuals within an organization, the cybercriminal aims messaging at high-level executives such as CEOs, CFOs, and COOs in order to trick them into revealing sensitive information and corporate data. These targets are carefully selected because of their access and authority within an organization.

In addition, users with no technological skill at all are able to engage in such activities using *phishing kits* and *phishing-as-a-service*. *Phishing kits* allow novices to purchase and run pre-built packages and *phishing-as-a-service* allows unskilled offenders to hire someone else to conduct the attack (Thomas et al., 2017).

Studies on phishing

Dhamija et al. (2006) conducted one of the earliest studies investigating why people fall for phishing scams, asking participants to identify various Web sites as legitimate or fake. They found that highly effective phishing sites fooled 90% of their participants and that most browser cues were opaque to these end-users. Victims did not realize that Web pages can be easily copied, and thus incorrectly judged these sites based on their content and their professional appearance. Downs et al. (2006) conducted a complementary study examining phishing e-mail messages that replicated the Dhamija et al. (2006) study, finding that participants used basic and often incorrect heuristics in deciding how to respond to e-mail messages. For example, some participants reasoned that since the business already had their information, it would be safe to give it again. These early studies were largely atheoretical, focusing more on description than explanation.

More recent studies (Leukfeldt, 2015; Leukfeldt et al., 2016) explore the relationships among phishing and cybercriminal networks, social ties, and online forums. For example, research by Leukfeldt et al. (2016) found that social ties play an important role in the origin and growth of the majority of networks that criminals with access to forums are able to use to criminally exploit quickly and easily.

There are studies on *phishing* outside the field of criminology, which focus on education and training. Two studies by Arachchilage and Love (2013, 2014) tested the efficacy of security awareness. These studies showed a significant improvement of participants' *phishing* avoidance behavior after playing a game based on security best practices. Furthermore, the findings suggest that participants' threat perception, safeguard effectiveness, self-efficacy, perceived severity and perceived susceptibility elements positively impact threat avoidance behavior, whereas safeguard cost had a negative impact on it (Arachchilage & Love, 2013, 2014).

Studies on phishing and Routine Activity Theory

As mentioned above in the section on the suitability of Routine Activity Theory for digital crimes, there are few studies on phishing that utilize RAT (Hutchings & Hayes, 2009; Leukfeldt, 2014, 2015). Leukfeldt (2014) and (Leukfeldt, 2015) focus on *suitable targets* and *risk factors*, respectively. Leukfeldt (2014) finds that personal background and financial characteristics play no role in phishing victimization, that having up-to-date antivirus software as a technically capable guardian is an insignificant factor, and that no single, clearly defined group has an increased chance of being a victim. The study concludes that while *target hardening* may help, there are limited opportunities for prevention campaigns aimed at specific target groups or dangerous online activities, making situational crime prevention problematic. There is the suggestion that banks could play the role of capable guardian to potentially mitigate this shortcoming (Leukfeldt, 2014).

Leukfeldt (2015) also compares victimization risk factors for two types of phishing: high-tech phishing (e.g., using malicious software) and low-tech phishing (e.g., using e-mails and telephone calls). The findings show situational crime prevention has to be aimed at groups other than just the users themselves. Criminals are primarily interested in popular online places and the onus is on the owners of these virtual spaces to protect their users from being victimized from both high- and low-tech phishing (Leukfeldt, 2015).

Thus, at present, there remains a clearly-defined gap in our understanding of the utility of RAT to the prevention and control of phishing, which this study seeks to address. At present there are no widely-successful mechanisms, technological or human-focused, to prevent victimization through phishing. The current study seeks to further refine the results of past studies with different data and research questions regarding both the factors behind the evolution of *phishing* and the viability of RAT for guiding policies to combat this ubiquitous form of cybercrime.

Methodology

The study utilizes personal interviews as its data source. This research methodology allows for a deeper understanding of relatively new and undeveloped areas, and for consideration of prominent theoretical issues and policy concerns (Corbin & Strauss, 2008; Creswell & Poth, 2018). Questions were developed which could allow for a better understanding of how phishing may continue to evolve in the future, how it may be better combatted, and to examine both the utility and further development of Routine Activity Theory for cyber-crimes.

A qualitative study is appropriate when the goal of research is to explain a phenomenon by relying on the perception of a person's experience in a given situation (Stake, 2010). As outlined by Creswell (2014), a quantitative approach is also appropriate when a researcher seeks to understand relationships between variables. Because the purpose of this study is to discover relevant factors, both social and technological, to further-develop theory, and suggest control strategies, a qualitative approach is appropriate.

Research questions

In order to define the factors that lead to *phishing* enduring as a crime type and to refine the application of Routine Activity Theory to cyber-crime, and its prevention and control, the following questions were developed:

RQ1: What factors allow *phishing* to exist as a long-term, successful crime type?

RQ2: What *technological* solutions are viable both now and in the future?

RQ3: What *human-focused* prevention strategies are viable now and in the future?

Study participants

The overall sample (N = 62) was drawn through purposive sampling from three distinct, expert, and diverse populations in order to gain the broadest perspective in answers to the research questions: information technology/security professionals, "hackers," and academic researchers. The purposive sampling technique is the deliberate choice of a participant due to the qualities the participant possesses (Etikan, 2016). It is a nonrandom technique that does not need underlying theories or a set number of participants. With purposive sampling, the researcher decides what needs to be known and sets out to find people who can

and are willing to provide the information by virtue of knowledge or experience (Barratt et al., 2015). This involves identification and selection of individuals or groups of individuals that are proficient and well-informed with a phenomenon of interest. Unlike random studies, which deliberately include a diverse cross section of ages, backgrounds and cultures, the idea behind purposive sampling is to concentrate on people with particular characteristics who will better be able to assist with the relevant research (Barratt et al., 2015; Etikan, 2016), in this case, those with the most information on *phishing* and cyber-crime victimization.

Though the selected groups varied in age-range, years of experience, and other demographic factors (such as gender balance), the responses to interview questions were overwhelmingly similar. Due to the lack of any significant differences in responses, and the nature of the study (i.e., interviewees are the sources of information, not the object of study themselves), the groups were combined, providing one population for analysis.

The selection of respondents was dictated by the following two guidelines. First, participants must have worked, published, or participated in computer security for at least three years. Second, all participants had to be fluent in the English language, but English did not have to be their native language. Though the majority (N = 38) of interview subjects were based in the United States, there were a number of international participants (N = 24) as well.

Participants were recruited through existing professional networks of the researchers, the American Society of Criminology (ASC), and the Social Science Research Network (SSRN). Many of the participants had been interviewed for a previous project on international cyber-crimes and were willing to participate again. Initial contact for these participants was obtained for the prior project via "cold e-mails" and forum posts on popular cyber security websites such as "Krebs on Security" and "Naked Security."

The interview subjects were asked to respond via e-mail if they were interested in being interviewed on the topic of *phishing* or knew someone who might be. We informed the prospective participant that we hoped to interview approximately 20 people each from industry, enthusiast, and scholarly circles, that the interview would take approximately 30–60 minutes, and would be entirely confidential and anonymous. We initiated contact with 85 individuals and were able to interview 62 of them, for an overall response rate of 72.9%. This is similar to other comparable studies, such as the Leukfeldt research (2014, 2015), which both drew from the same data set at a 47% response rate and the Bossler and Holt research (2009), which had a response rate of 72.3%.

Data collection

A semi-structured, informal interview format was used, consisting of twelve open-ended questions that are in Appendix A. Interviews were conducted primarily by telephone (77.4%, N = 48) or video via FaceTime or Skype (12.9%, N = 8). A number of participants from the hacker group preferred to respond via text, either through e-mail or IRC (9.6%, N = 6). Written or verbal informed consent was provided by each participant before the interview. Each interview was conducted in a single session, and transcribed and coded for each specific question by the primary researcher.

Saturation (Glaser & Strauss, 2009) occurs when the researcher realizes that for a given subject, no new categories emerge from coding responses and therefore, nothing more can

be added to the data. It was possible that saturation could occur in this research. Once saturation is reached, the theory or phenomenon is said to be grounded in the data (Charmaz, 2006; Urquhart, 2013). Saturation was realized in this study after the 45th interview, and at that point one group (academics) was underrepresented in the sample. Interviews were continued in order to enhance validity by providing more equal representation among the initial groups selected for the study.

Data analysis

Coding of transcripts was completed in the order of the interviews conducted. Codes were created during the research process (Urquhart, 2013). Coding was conducted both manually by the lead researcher, and through computer-assisted qualitative data analysis software (NVivo 12). To test the reliability of the coding process, we utilized an inter-rater reliability check; the co-researcher coded a subset of the interviews (18 of the 62 total; 6 from each participant sample group) to compare to the lead researcher's codes. The process of analyzing, reanalyzing, and comparing new data to existing data is known as constant comparison (Birks & Mills, 2011; Urquhart, 2013). As each phase of coding began, the lead researcher reviewed the data collected in previous phases in order to see when saturation might be reached. Coding terminology followed the three-stage protocol developed by Glaser and Strauss (2009); open, axial, and selective/theoretical.

In the first phase of open coding, each line of interview text was transcribed resulting in numerous descriptive categories of response. Axial coding was then used when there were no new open categories, or when responses related only to the core categories that emerged in the interviews. Finally, selective/theoretical coding was conducted, comparing codes and categories that emerged during open coding and axial phases, where relationships were found among the previously established categories (Urquhart, 2013).

An example of this coding process is as follows for the first research question, "*What factors allow phishing to exist as a long-term, successful crime type?*" First, lines of dialog pertaining to *phishing* attack type were open-coded using respondents' own words, such as "simple/smart," "old/new," and "net/spear." Next, axial coding collapsed these related terms into concepts, "wide" (simple, old & net) and "narrow" (smart, new & spear). Finally, selective/theoretical coding integrated these conceptual codes to the "core concepts" of Routine Activity Theory, in this case *access*, an attribute of the *suitable target*. Though this process allows for new theoretical creation, our aim was to relate any relevant codes back to the established Routine Activity Theory.

Another example using the second research question, "*What technological solutions are viable now; and in the future?*" illustrates how some codes did not change through the coding process and were difficult to link back to theoretical "core concepts." Dialog mentioning "deepfakes" did not vary in the same way that dialog describing *wide* or *narrow* attack vectors did; the term *deepfake* is specific and does not cover a range of inter-related concepts. The axial code *phishing tool* does not add explanatory power, as no other *phishing tools* were mentioned by respondents. Likewise, neither code (*deepfake* nor *phishing tools*) provided a logical connection to a theoretical "core concept" of Routine Activity Theory, as the theory describes what factors may produce crime, but not how.

Findings

The findings to the questions are reported in the order they were presented to the interviewees, and include all the discovered codes for each question. The resulting codes were: (1) *wide* and *narrow attacks*; and *motivation*; (2) *technological proficiency differential* (TPD): and (3) *target value* (TV) for **RQ1**. For **RQ2**, they were: (1) *machine learning* and *multi-factor authorization*; (2) *human weakness*, and (3) *ransomware* and *deepfakes*. (1) *Target training* and (2) *target testing* were the only two relevant codes for **RQ3**.

RQ1: *What factors allow phishing to exist as a long-term, successful crime type?*

Nearly all participants (87%, N = 54) bifurcated *phishing* attacks, though the verbiage varied. These were coded as "*wide*" and "*narrow*," and had been labeled by the respondents in similar terms: "simple/smart," "old/new," and "net/spear."

"Wide" attacks

Wide attacks target large swathes of potential victims using low-effort and easily-defeated forms of *phishing*, primarily via e-mail, but increasingly via text (*smishing*) or phone (*vishing*). These attacks aim for the most easily gullible victims and the expected return rate is in decimal percentages. A consensus emerged from the interviews around the idea that these techniques are antiquated and unlikely to work well in most markets (79%, N = 49). One IT professional's response exemplified this view:: "*We all still get the occasional SPAM text and some of those SPAM texts are phishing attempts. But even my mom knows not to click on unsolicited links anymore, let alone give away the information phishers are looking for*" (IT#8).

"Narrow" attacks

Narrow attacks target specific groups or individuals using high-effort and complex forms of *phishing*, still primarily via e-mail, but incorporate relevant information to make the source of the attack more believable and the likelihood of success higher. Data from the FBI's Internet Crime Complaint Center (IC3) in 2019 reveals 23,775 complaints about Business E-Mail Compromise (BEC), which resulted in more than 1.7 USD billion in losses (Gorham, 2020).

A hacker's response regarding experiences with friends who have used BEC in the past said: "*These scams typically involve someone spoofing or mimicking a legitimate e-mail address. For example, you'll get a message that appears to be from an executive within your company or a business with which that person has a relationship. The e-mail will request a payment, wire transfer, or gift card purchase that seems legitimate but actually funnels money directly to a hacker*" (H#23).

Spear phishing and *whaling* attacks are also narrow attacks, though they are deployed with the less frequency than BEC because they require more up-front effort from attackers. Most "whales," such as CEOs, are insulated to e-mails from the general public; their e-mail addresses typically are not publicized, customizable software filters stop whatever is undesired, and many of these intended victims have an assistant to deal with their e-mail for

them. However, a phishing attempt that can circumvent or penetrate these conditions may lead to a very large payout. As one academic respondent (AR#4) noted: *"You have to assume these are happening more than we hear about. What CEO wants to admit they've been duped?"* This in turn affects the issue of "non-issue making," (Crenson, 1972) or the tendency for corporations and governments to hide criminality *and their victimization* for fear of appearing weak, organizational sanctions against them, and, necessarily, increases their risk future victimization.

While earlier studies have utilized Routine Activity Theory (RAT) to identify factors causing a target's victimization, none have analyzed why those factors persist through time. In the categorization created in this study (wide vs. narrow), we can see that *phishing* has not remained the same and that the crime has changed, in both method and target.

When asked **RQ1** directly, the answers all took the wide vs. narrow distinction into account, producing three additional factors, coded as: *motivation, technological proficiency differential (TPD)*, and *target value (TV)*.

Motivation

Profit, or stealing things of monetary value, is the overwhelming motivational factor for *phishing* attacks (Egan, 2020; Gorham, 2020) and although the number of targets and means of targeting may change, this economic motivation has remained constant. Every respondent (100%, N = 62) cited money as the primary motivation for *phishing*. Beyond this, a number of participants mentioned non-monetary targets that produce motivation, such as nude photos of celebrities, a topic which will be covered in more depth under *target value*.

One hacker (H#18) made a novel comparison concerning relative risk for various cybercrimes: *"Back in the day, you could deface websites for fun. They'd notice and fix it. You had your fun and maybe ruined a guy's afternoon, but no one was out millions of dollars and you're not looking at a possible felony charge. Now, if you're committing a crime online, you're doing it for a reason. And what better reason is there than money?"*

Technological proficiency differential

There remains a large difference in the technical capabilities between the average hacker and the average internet user. As respondents noted: *"Who is better with a computer, you or your mom? You, younger by definition. Who is more likely to be doing the phishing? The younger person. And who is targeted? The older one,"* (H#13) and *"It's the difference between pro-MMA (mixed martial arts) and backyard boxing. The guy coming at you does this for a living and you use your computer for fun"* (H#6).

This *technological proficiency differential* (TPD) is always present, even if it varies between offenders and victims. One academic researcher (AR#1) points to this as one of the defining problems for victims of *phishing: "No one secured their Wi-Fi. Wireless routers used to ship without encryption on by default, and no amount of public service announcements or scary news stories got anyone to change their behavior. So, the router companies just started shipping them with encryption on. Now the problem is that no one changes the default password. We've kicked the can down the road. Solved the first problem, but people are always going to be lazy."*

Target value

Though *wide attacks* are still most prevalent, the increased use of *narrow attacks* presents an opportunity to analyze a new type of *suitable target*. In order for one victim to "replace" many, the target has to be worth more in order to provide comparative rewards to criminals. If a net catches hundreds of "salmon" for a worthy payout, one *whale* needs to be comparable in size. The reward does not necessarily need to be monetary; more than half of the participants (53.2%, N = 33) drew attention to the widely-publicized 2014 *phishing* case known colloquially as "Celebgate."

On August 31, 2014, a collection of approximately 500 nude pictures of various celebrities, mostly women, were posted to an online imageboard (Ohlheiser, 2016). The pictures were initially believed to have been obtained via a breach of Apple's cloud services suite iCloud, or from a security issue in the iCloud API that allowed attackers to make unlimited attempts at guessing victims' passwords. However, access was later revealed to have been gained via *spear phishing* attacks. Court documents from the case explain that the perpetrator created a fake e-mail account called "appleprivacysecurity" to ask celebrities about their security information (Ohlheiser, 2016). This further underscores a long-standing finding from major studies that the easiest way into a computer is usually the "front door" (Rosoff et al., 2014).

Participants stated that this case, represented a "perfect storm" for a *spear phishing* attack. That is, the suitable target is extremely rare (compromising photos of a particular celebrity), the capable guardian is at a technological disadvantage, and the offender is able to collect public data about the celebrity's life in order to craft a targeted e-mail that is believable.

Many of the factors described above are present in other forms of cyber-crime and are not unique to *phishing*, for example, *motivation* and *target value* are both present for website defacement. In these cases, the *motivation* is non-monetary, usually fame, and *target value* is based on visibility (Howell et al., 2019). Assuming more people are motivated by money than fame, or are more willing to risk a prison sentence for money than fame, we expect crimes such as *phishing* to out-pace crimes such as website defacement.

RQ2: *What technological solutions are viable now; and in the future?*

There were only two relevant solution codes for this research question, both of which had near complete (96.7%, N = 60) or complete frequency (100%, N = 62), respectively: *machine learning (ML)* and *multi-factor authentication (MFA)*. Another code had complete frequency (100%, N = 62), though it is not a solution, but rather a condition: *human weakness*. A follow-up question asked the interviewee to anticipate any growing problems for victims of *phishing*; two prominent codes emerged, *ransomware* and *deepfakes*.

Machine learning

The majority of participants (96.7%, N = 60) mentioned "AI" (artificial intelligence) or "ML" (machine learning, a subset of AI) as both an immediate and long-term solution. Studies on machine learning and phishing report a 97.98% accuracy rate for detection of phishing URLs for real-time and language-independent classification algorithms (Sahingoz

et al., 2019). The major caveat, however, is that this type of detection only works on *wide attack* campaigns that are being replaced by the hard to humanly or machine-detect, *narrow attack* campaigns, such as Celebgate.

Just as unsolicited, bulk e-mail ("spam") has largely been defeated by automated inbox filters, participants believed ML algorithms would solve the *wide attack* vector of *phishing*. As one academic respondent described, *"Spam filters are garbage disposals. ML is 'The Terminator'"* (AR#10). There were far fewer participants (%/N) who believed machine learning would be a panacea for more sophisticated attacks. *"Nothing has passed the Turing Test, as far as I'm aware, and if [AI] can't fool us, why shouldn't we expect to fool it?"* (H#19) and, while that logic might not be sound, the sheer complexity of the issue remains valid. Machine learning depends on "big data" (patterns derived from large datasets) and *spear phishing* attempts are relatively rare for reasons discussed earlier.

Multi-factor authentication

Multi-Factor Authentication (MFA) is a secure identification method by which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism, such as knowledge (something only the user knows), possession (something only the user has), or inherence (something only the user is). *Phishing* attempts can only extract *knowledge*, not *possession* nor *inherence*. By enabling MFA, all participants claimed successful *phishing* attempts can be significantly negated or detected.

Human weakness

It is important to note that while most interviewees agreed that machine learning (96.7%, N = 60) and multi-factor authentication (100%, N = 62) were solutions for most *wide*, and some *narrow* vectors, all participants (100%, N = 62) repeated a variation of "there is no technical solution for every *human weakness*." Those weaknesses make even the best technological solutions incomplete and are covered in more depth under the findings for the next research question.

Two codes emerged suggesting present and future technological problems as well; these are *ransomware* and *deepfakes*.

Ransomware

Ransomware is a type of malware that threatens to perpetually block access to a user's data unless a ransom is paid (Brewer, 2016). It uses a technique called "cryptoviral extortion," in which malware encrypts the victim's files making them inaccessible; the offender then demands a ransom payment, usually in the form of untraceable cryptocurrency, such as Bitcoin, to decrypt the files for user-access (Mansfield-Devine, 2016a). The most frequent delivery method for *ransomware* is *phishing* (Egan, 2020; Gupta et al., 2018).

Ransomware is not a new problem, but one that many participants (66.1%, N = 41) believed was not part of the *phishing* discussion and should be. One IT specialist (IT#15) noted, *"According to the best data out there, ransomware costs corporations in one year what phishing costs them in three. The phishing costs don't include ransomware costs, even though*

phishing is the most common attack vector for ransomware." Others expressed similar thoughts, with varying levels of exasperation: *"Tell me how someone gets ransomware without clicking something they shouldn't have. Phishing is all about getting people to do just that"* (H#6).

Deepfakes

Deepfakes are synthetic media in which a person in an existing image, video, or audio file is replaced with someone else's likeness (Stupp, 2019). While the act of faking content is not new, deepfakes leverage powerful techniques from machine learning to manipulate or generate visual and audio content with a high potential to deceive. About half the interviewees (51.6%, N = 32) mentioned deepfakes as a possible *phishing* issue. One IT professional (IT#10) said, *"Can you imagine getting a realistic-sounding and angry-seeming voicemail from your 'boss'? The success rate on that type of attack would be near one-hundred."*

Other researchers (91.9%, N = 57) were quick to offer an alternative future (AR#3): *"They fool people better than machines. This is an example where machine learning will help as much as hurt. The most popular technique for detection is to use algorithms similar to the ones used to build them to detect them. By recognizing patterns in how they are created, the algorithm is able to pick up subtle inconsistencies. People have developed automatic systems that examine videos for errors such as irregular blinking patterns of lighting already."*

RQ3: *What human-focused prevention strategies are viable now; and in the future?*

Continuing the theme from the previous research question, one hacker (H#15) mused, *"You have to be vigilant every time you open an e-mail, fill out a form, or click a link. I just need you to mess up once."* Technological solutions, interviewees agreed, can stop most *wide* attacks and, perhaps, some of the *narrow* ones as well, but there will invariably be ones that get through to the targeted end-user. The suggested *human-focused* solutions were coded as *target training* and *target testing*.

Target training

Research shows that people can be trained to recognize phishing attempts, and to deal with them through a variety of approaches (Arachchilage & Love, 2013, 2014). Such education can be effective, especially where training emphasizes conceptual knowledge and provides direct feedback (Arachchilage & Love, 2013, 2014). The problem, many (88.7%, N = 55) participants noted, is that most corporations treat *"cyber security like a joke and want to spend as little as possible on it, including optional trainings they know will be ignored"* (IT#2) and *"there's no cyber security training at all for people outside of Fortune 500 companies"* (IT#17). As a result, a number of respondents (69.3%, N = 43) believe cyber security education is currently inadequate. Some interviewees (45.1%, N = 28) noted that nearly all legitimate e-mail messages from companies to their customers contain an item of information that is not readily available to *phishers*, but that "no one" knows this. Again, this solution is of limited effectiveness against *spear phishing* attempts where attackers research their targets well and can utilize the collected information accordingly.

Interestingly, about half of the respondents (48.3%, N = 30) noted two subsets of end-users where training would be "worthless." First, end-users that were so technologically proficient that they were functionally "immune" to *phishing* and did not need additional training. Second, end-users that were so technologically inept that they were "immune" to training and would fall victim to attacks no matter what.

A number of interviewees (32.2%, N = 20) shared personal anecdotes such as, *"The people I know who are best about this stuff are the people who were previously victimized"* (AR#13) and *"The ones who never speed are the ones who got caught speeding before . . . "* (H#20). These off-hand comments stress the importance of the next code, *target testing*.

Target testing

Many organizations run regular simulated phishing campaigns targeting their own staff to measure the effectiveness of their training (Whitaker & Newman, 2006; Wilhelm, 2013). Those that fall for the simulated attempt are given additional training, with anecdotal evidence that repeat offenders sometimes have e-mail access temporarily revoked. A few hackers (20%, N = 13) semi-joked that *target testing* could be improved by adding an element of shame: *"This problem would fix itself real [sic] quick if Jerry in accounts receivable was put on a public Hall of Shame list each time he clicked on a fake link"* (H#11). Interestingly, research on other white-collar crimes, such as embezzlement, demonstrates public shaming can have an effect on *offenders* (Braithwaite, 1989; Kahan & Posner, 1999; Murphy & Harris, 2007). Whether or not it would have an effect on victims remains to be seen. Even if it proved to be an effective solution, the morality of it is questionable at best.

Discussion

The goals of this study were to provide an overview of *phishing* in the present, reveal the factors that allow it to persist, suggest solutions to combat it, and to update the application of Routine Activity Theory to cyber-crimes.

Wide-net *phishing* remains the most common form of *phishing*, but *spear phishing* has grown in popularity since approximately 2010, especially against extremely high *target value* infrastructure. In 2011, staff at defense contractor RSA were successfully phished, which lead to the master key for all "RSA SecureID" security tokens being leaked (Richmond, 2011). These security tokens are utilized by all officials at the U.S. Department of Defense for multi-factor authentication. Two years later, all U.S. Target stores fell victim to an attack that occurred after a successful phishing attempt against the company's contracted heating and ventilation supplier (Kassner, 2015). There are numerous examples of similarly costly phishing attacks: Ubiquiti Networks lost 46.7 USD million in 2015 (Krebs, 2015), FACC Aerospace lost 55 USD million in 2016 (Nasralla, 2016), Crelan Bank lost 75.8 USD million also in 2016 (Schneider, 2016), and Google and Facebook lost a combined 100 USD million in 2017 (Romo, 2019).

These recent cases demonstrate a need for studies such as this one, which attempt to answer questions about the current state of *phishing* attacks, what can be done to increase security, and provide a guide for future theoretical development.

Phishing evolves and survives

This responses to our first research question suggest that the factors that allow phishing to adapt as a crime type and persist through time are *motivation, technological proficiency differential (TPD)*, and *target value*. Routine Activity Theory (RAT) assumes there is always a *motivated offender*. Past cyber-crime studies (Grabosky, 2001) have likened connecting to the internet to "opening a front door," (Rosoff et al., 2014) as it allows access to both legitimate and criminal parties. Our study did not attempt to answer the question "Why utilize *phishing* over other types of cyber-crime?" rather, what allows *phishing* to persist. The answers provided by our respondents fit within established Routine Activity literature (Clarke et al., 1999; Cohen & Felson, 1979; Leukfeldt & Yar, 2016; Yar, 2005) given they believe shifting *motivations* have resulted in a growth of *phishing* attack types, such as *spear phishing* and BEC. If these new types become less successful, as has happened for *wide* "net" attacks, we expect the *motivational* calculus to change and offenders to move to "greener pastures," possibly other types of cyber-crime.

As the primary *motivation* is monetary, successful attacks are those that adapted appropriately to follow the money; technological advances have more or less solved the *wide* approach, making these attacks less successful, so the motivated adapt and try the *narrow* approach instead. To justify the greater investment of time involved, targets are hand-picked. If there is potential financial gain through some form of *phishing*, there will be hackers willing to do it.

This study also suggests that a *technological proficiency differential* (TPD) may allow *phishing* to continue to succeed as a form of cybercrime through relative diminution of the *capable guardian* condition of RAT. For an attack to succeed against a corporate target, the *phisher* must make it past a number of industry-standard protections, including ISP-level filtering and custom corporate firewalls, plus the detection of the (likely trained, to some degree), targeted user. In this corporate case, ultimate detection is up to the end-user, but an attacker must first successfully navigate the protections installed by IT professionals that are likely to have a low TPD in relation to the offender. The IT department is close in abilities to whichever hacker may target the corporation and it ordinarily takes *target hardening* steps to protect the corporation from its employees and others. For an attack to succeed against a home user, however, the *phisher* must only make it past the number of protections the end-user is aware of and able to implement. As noted earlier, Wi-Fi encryption illustrates this point. Corporations were aware of and implemented Wi-Fi encryption early in its introduction, while individual households only began to adopt the protection when router companies turned the measure on by default (Gold, 2011).

For end-users to adequately protect themselves against *phishing* at home, they must be aware of and capable of properly configuring the following: a modem, a router, a firewall, an adblocker, a password manager, and multi-factor authentication. Moreover, they must know what *phishing* is and be able to detect it, in order to avoid victimization. As one interviewee (AR#17) put it, *"It's not even a manner of being lazy or ill-informed, how do you possibly keep up with the rate of advancement?"*

Phishing has evolved to the point where successful attacks are those that can circumvent the target hardening technology of corporations, as in carefully-tailored *whaling* messages, or that can evade the detection of uninformed users, such as in the case of business e-mail compromise (BEC).

Again, the goal of this research question was not to provide reasons *phishing* is utilized over other cyber-crimes, but the discussion with respondents suggests *phishing* might be a simple way of achieving their goals, which may be why some offenders use it. In the 2014 "Celebgate" case, for example, journalists originally assumed the hack was done through API vulnerabilities (Ohlheiser, 2016). This is a more complex task, requiring a hacker to test their abilities against Apple engineers instead of end-users, a situation where the offender may have a TPD deficit in relation. Ultimately, it was discovered that Celebgate was a "simple" *spear phishing* attack (Ohlheiser, 2016).

The final factor that our study suggests allows *phishing* to persist as a successful crime type is *target value*. Past studies have operationalized the *suitable target* portion of RAT using acronyms to describe accessibility: VIVA (Value, Inertia, Visibility, Access) (Cohen & Felson, 1979) and CRAVED (Concealable, Removable, Available, Valuable, Enjoyable, Disposable) (Clarke et al., 1999). Our research indicates digital accessibility is similar to physical accessibility, at least for *phishing*. Though we only received responses addressing the *target value* portion of VIVA and CRAVED, it is apparent that digital data is also easily concealable, easily removable, widely available, and easily disposable. As ISP-level e-mail filtering has become standard, the low-hanging fruit have been lessened, and the *phishing* community has responded by targeting things of ever-increasing value. Participants mentioned the 2014 "Celebgate" case, but the 2017 "Vault7" hack provides a more illustrative example of this phenomenon.

Vault7 is a series of documents that WikiLeaks began to publish in March of 2017, that detail the activities and capabilities of the United States' Central Intelligence Agency to perform electronic surveillance and cyber warfare (Barnes, 2020). The files, dated from 2013–2016, include details on the agency's software capabilities, such as the ability to compromise cars, smart TVs, web browsers, and the operating systems of most smartphones.

A CIA internal audit identified 91 out of more than 500 malware tools in use in 2016 being compromised by the Vault7 release (Barnes, 2020). The report detailed a wide range of security flaws that lead to the leak, mainly, that the intelligence community has yet to protect its.gov domain names with *multi-factor authentication*; and, the CIA, National Reconnaissance Office, and National Intelligence office have yet to enable *DMARC*[1] *anti-phishing protections*.

In both the Celebgate and Vault7 cases, the target *suitability* is determined almost exclusively by the *target value*. There is presumably a larger market for stolen nude photos of women than men, as during the initial release of stolen Celebgate photos, there were approximately 100 female victims and less than ten male ones. Likewise, while all major governments presumably have hacking tools that criminals desire, the U.S. is widely-known to have the world's largest collection of zero-day exploits (Smith, 2013; Zetter, 2014).

The Target retail store phishing example also demonstrates allowances can be made for inertia, visibility, and access, so long as the target is of high enough value. The heating and ventilation company that fell victim to the initial attack and provided a vector into Target's larger network is relatively small and only licensed to work in five states (Harris, 2014; Kassner, 2015).

The findings regarding *target value* suggest they may dictate which form of cyber-attack the offender chooses to utilize. The Celebgate example mentioned by about half of the participants (53.2%, N = 33) is not easily achievable via other means. A man-in-the-middle

attack would have required the target images to be caught during transmission, something which is not guaranteed to occur (Hutchings et al., 2015). Ransomware does not work if the victim is willing to lose the data encrypted by the attack (Malecki, 2019). A brute-force attack on Apple's iCloud API may have worked, and was originally assumed to be how the hack occurred, but would have been more time- and skill-intensive than *phishing* (Ohlheiser, 2016).

Technological solutions are effective, yet imperfect

Our second research question addresses the ability of technology alone to act as a *capable guardian*. There are a wide range of solutions that have been implemented to varying success through the past two decades, most recently: Google's Safe Browsing URL blacklist (used by Chrome, Safari, and Firefox) and DMARC (used by Bank of America, Fidelity Investments, and JPMorganChase, among others). These can currently block many, but not all *phishing* attempts. Our research suggests two technologies can further protect average end-users. First, studies repeatedly demonstrate *machine learning* has a 95+% success rate at blocking *wide attacks* (Sahingoz et al., 2019). Second, *multi-factor authentication* offers not only additional protection against being successfully *phished*, but also notifies potential victims of *phishing* attempts (Kennedy & Millard, 2016).

Neither of the above solutions, however, protect against *spear phishing*. Though still less-frequent than traditional *phishing, spear phishing* attacks are increasing in popularity. One reason relates to the idea of *system capacity*, which is undoubtedly at play, as the types of crimes that succeed are those to which the current enforcement apparatus is unable to effectively respond (Pontell, 1982; Pontell et al., 1994). Routine Activity Theory suggests that *ML* and *MFA* are valid *target hardening* techniques for *wide*, but not *narrow* attacks. Unlike non-digital crimes, where potential victimhood occurs simply by being in contact with others, the technology necessary to adequately harden against *spear phishing* must also be able to save an end-user from themselves.

Our analysis produced two important related factors, which various people believed are current and growing problems emanating from phishing: *ransomware* and *deepfakes*. *Ransomware* is an immediate financial issue as it is currently the source of billions of dollars of damage to corporations yearly (O'Neill, 2020) and there remains no lasting technological solution. Ransomware has been widely researched as a cyber-crime, but there remain few studies that analyze links between ransomware and phishing, even though official statistics show ransomware is most commonly delivered as a *phishing* payload (Egan, 2020). *Deepfakes* appear to be a growing problem as well (Pantserev, 2020; Wojewidka, 2020), but most interviewees (91.9%, N = 57) believed the technology to detect deepfakes was progressing at much the same rate as the technology to produce them. Deepfakes as a crime tool have also been widely researched, primarily in relation to the production of fraudulent political videos and pornography, including fake celebrity sex videos (Maddocks, 2020; Öhman, 2020). There remain no studies of the interrelationships between deepfakes and phishing to date, although this may be due to the relative infancy of the combination of these cybercrimes, and a corresponding lack of data.

Regarding end-users and current solutions, our respondents believed that those most informed on *phishing*, and most *technologically proficient*, are the end-users that are in least need of technological solutions. For example, advanced computer users are both more likely

to run adblockers and more likely to avoid clicking on any ads that might slip past the blocker.

The study results suggest that the types of *phishing* that have grown in popularity (*spear, whale*, BEC, etc.) are those that primarily bypass the human element of *guardianship*. Though these tend to also bypass technological solutions, they are designed with the end-user in mind and continue to succeed as a result. For example, SPAM has been almost entirely solved through the blocking of automated mass-e-mail (slowing the outward flow of SPAM) and shared blacklists (culling the inward flow of SPAM) (Crawford et al., 2015). Both of these are technological solutions with no level of human involvement. Likewise, direct human involvement was removed from the Wi-Fi encryption process when manufacturers started shipping routers with the protection on by default (Gold, 2011).

There currently is no effective way to entirely remove the "human" part of replying to an e-mail, text message, or phone call. Attacks that are personalized are especially likely to succeed by lowering user inhibitions through faux familiarity. And, though there is no way to entirely remove this human part of the risk, the final research question suggests ways to ameliorate it.

Teach, then test, and repeat, if necessary

The final research question addresses the measures necessary to produce the *capable guardian* as a human element. "Education" is a frequently offered, nebulous solution to complex issues such as cyber security, and it very well may be, but the finer details are often absent from the discussion (Arachchilage & Love, 2013, 2014). Respondents in this study agreed that proper training could reduce the vast majority of successful *phishing* attacks. The types of training suggested varied, but typically included "awareness" (what *phishing* is) and "prevention" (how to recognize it). The participants with industry experience did not generally believe that current programs were adequate (69.3%, N = 43).

Vulnerability assessment is the process of identifying, quantifying, and prioritizing the weaknesses in a system. They are performed on systems of information technology, energy supply, and communication, among others. The General Services Administration (GSA) has standardized "Risk and Vulnerability Assessments" (RVA) as a pre-vetted support service. This service conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. This standardized service offers many pre-vetted support services, but relevant to this discussion are Network Mapping, Vulnerability Scanning, and Phishing Assessment.

As part of these assessments, corporations or agencies are tested with a penetration test. A "pen test" is an authorized, simulated cyberattack on a computer system, performed to evaluate the security of that system, which can include *vishing, smishing*, and *phishing* attempts. As these are customized to the corporation or agency being tested, they accurately mirror real-world *spear phishing* attempts. Our study found that these are widely believed to be successful and worthwhile. It is a pro-social way of simulating victimhood that promotes learning and an adaption of future behavior. Some of the participants (20.9%, N = 13) also argued that they believed these assessments would be more effective with an element of shaming. This is beyond the scope of Routine Activity Theory and, thus, this study, but might be worthy of future research.

A final noteworthy result is that about half of the interview subjects (48.3%, N = 30) believed that certain end-users, perhaps the interviewee themselves, were functionally immune to *phishing*. They believed that these users were *technology proficient* enough that the *differential* was in favor of the target and not the *phisher*. Likewise, these participants felt that a countervailing population of end-users were immune to *training* and were almost guaranteed victims, if they were to be targeted. The remaining majority of people presumably fall somewhere in-between these two extremes, where the need for training and the benefits from it intersect.

Limitations

This study includes a number of limitations due to its nature as an interview-based, qualitative, and cyber-focused research project. Interviews are costly, time-consuming, and vulnerable to interviewer bias. These issues were addressed by conducting all interviews via voice or video, limiting sessions to roughly 45 minutes, and fully informing interviewees of our positions, affiliations, study aims, and general methodology. Qualitative research is also more vulnerable to sampling and self-selection biases. While it is possible our purposive sample has produced erroneous results, the resulting data saturation in this study leads us to believe that the information is accurate barring the rather unlikely prospect that the IT professionals, hackers, and academic researchers all offered intentionally false, yet overlapping responses. The possibility remains, however, that the interview subjects who participated (72.9%, N = 62) are significantly less-informed than those who did not (27.1%, N = 23). A demographic background study of all potential participants could address this, but was not feasible in this research, and self-selection bias existing to any significant degree is highly unlikely in any case. Lastly, while data availability for cyber-crime are increasing, there remains a noticeable lack compared to other subfields of criminology. Other studies on *phishing*, for example, have many of the same limitations listed here, or worse (Yang et al., 2015). For example, samples drawn from a population consisting entirely of college students are common (Bossler & Holt, 2009; Downs et al., 2006; Sun et al., 2016).

Future research

Our results suggest a number of avenues for future research. First, we believe *motivation, technological proficiency differential (TPD)*, and *target value* warrant more operationalization and quantitative study. TPD, in particular, is a factor that has potential explanatory power for a wide variety of cyber-crimes beyond phishing, including malware and ransomware victimization. Second, additional studies need to be conducted on the efficacy of *training* and *testing*. To date, there are no studies that we were able to locate on *phishing* education that use an experimental methodology. Third, Braithwaite's (1989) reintegrative shaming has been shown to be effective in the case of petty crimes, and past studies suggest shame also works for white-collar offenders as well (Kahan & Posner, 1999; Murphy & Harris, 2007), so the suggestion offered by respondents in this study for training that involves "shaming" for victims may also merit further study in the field of cybercrime in general.

Conclusion

Respondents in this study generally agreed with the notion that technological advances increase the proliferation of phishing attacks, but also aid in their detection. It has never been easier to conduct a simple attack, but a good attack requires more effort than ever before. Second, while phishing was viewed as directly responsible for a significant amount of financial fraud, it causes even more damage indirectly, as the primary attack vector for ransomware. Third, newer types of attacks utilizing technology such as deepfakes may make the problem worse in the short-term (Stupp, 2019). Fourth, prevention and enforcement will be derived primarily though machine learning and public education.

In sum, simpler forms of *phishing* have been relatively contained through technological efforts, similar to the removal of SPAM through filtering and the forced-adoption of Wi-Fi encryption. More targeted forms of phishing are unlikely to be halted by technology, and will continue to succeed if human-focused efforts, such as education, are lacking or non-existent.

Finally, the results show the utility of Routine Activity Theory as applied to *phishing* and cyber-crime analysis more generally with some modification, including the *technological proficiency differential* as a factor in cybercrime victimization. We believe the critiques of the application of Routine Activity Theory are valid (Leukfeldt & Yar, 2016; Yar, 2005), but perhaps overstated. The asynchronous nature of cyber-crime, for example, is not theory-breaking if we allow the "convergence" to be between victim and *phishing* e-mail, rather than between victim and the offender themselves. Likewise, we do not believe "location" and "distance" translate perfectly from real-world to digital, but do believe treating a user's e-mail inbox as the "scene of the crime" is appropriate.

Policy implications

The policy implications of this study are helpful, if bleak. The responses to the first research question, "What factors allow phishing to exist as a long-term, successful crime type?" provide meaningful guidance for future policy. The primary *motivation* for *phishing*, money, has remained constant, even as the targets have shifted from *wide* to *narrow*. Corporations and individuals cannot reduce the "benefit" (payout) of a successful *phishing* attempt, but it can increase the "cost" (security) of doing so. Increased security measures in the form of firewalls or multi-factor authentication, for example, are not guaranteed to keep an intruder out of a target system, but may deter them enough that they search for more easily-breached infrastructure. A few respondents (14.5%, N = 9) mentioned old joke-turned-security-adage: *"You don't have to swim faster than the shark, you just have to swim faster than your friend."* While we believe these deterrence measures would be effective at the individual level, studies have demonstrated increasing legal penalties at the governmental level may not have a similar effect (Forst, 1983; Herath & Rao, 2009; Scholz, 1997). In fact, the U.S. governmental response to cyber-crime, the Computer Fraud and Abuse Act of 1986, is routinely criticized for being too punitive already (Green, 2013; Wu, 2013).

Related to *motivation* is *target value*. As our lives have become more digitized, the likelihood that a compromised computer or account contains something of value has increased. Until the advent of the smartphone, photographs, including scandalous ones, were physical, likely hidden, and difficult to steal. The "Celebgate" case of 2014 is not only

an example of a widely successful *phishing* attack, but also an example of a new type of *valuable target*. In the United States, there have been no policy proposals to protect these new types of data, and over the past decade, governments worldwide have decried the increased use of encryption by the public for fear of "going dark" and losing access to devices which may contain evidence of criminal activity (Bellaby, 2018; Weimann, 2016). Policy proposals to deal with "going dark," including the Lawful Access to Encrypted Data Act (LAEDA), seek to provide "backdoor" access potentially opening a new avenue of attack for savvy *phishers* (Crocker, 2020).

Addressing the *technological proficiency differential* is one area we believe public policy may have a large effect. In response to the third research question, *"What human-focused prevention strategies are viable now and in the future?"* many respondents (88.7%, N = 55) called for increased educational efforts or *training*. Many public schools require "typing" courses; including a unit on cyber security best practices could have wide-reaching and long-lasting effects. There has also been a concerted effort to include computer coding as part of school curriculum, which would reduce the *technological proficiency differential* between offenders and the general population, so addressing security in this context also makes sense.

The responses to the third research question also included references to *testing* and *shaming*. Under current U.S. law, most corporations are not required to conduct security audits, report breaches, or follow best practices. Three industries are currently regulated under federal law: healthcare organizations (via the 1996 Health Insurance Portability and Accountability Act), federal agencies (via the 2002 Homeland Security Act), and financial institutions (via the 1999 Gramm-Leach-Bliley Act). In 2012, two U.S. senators proposed the Cybersecurity Act, which failed to pass (Rizzo, 2012). Supported by the military and the president, the bill would have required creating voluntary "best practice standards" for protection of key infrastructure from cyber-attacks, which businesses would be encouraged to adopt through incentives such as liability protection. The opposition claimed the bill would introduce regulations that would not be effective and could be a "burden" for businesses (Rizzo, 2012). Nearly all respondents (69.3%, N = 43) mentioned a necessity for best practices, including *testing*, and some wondered about the efficacy of *shaming* (20.9%, N = 13). Though governments have used shaming in the past, historical examples include stocks and pillory, we do not believe this is something governments will (or should) do.

Lastly, returning to the second research question, *"What technological solutions are viable both now and in the future?"* we expect technological solutions will be created and willingly adopted by actors with vested interests in security. For example, Google's Safe Browsing URL blacklist (used by Chrome, Safari, and Firefox) and DMARC (used by Bank of America, Fidelity Investments, and JPMorganChase), allow corporations to provide increased security with low barriers to entry. In the future, government bans on *deepfakes*, at least within the political realm, seem likely, and technology will be the most efficient way to detect these fake videos.

We believe our findings show any and all technological solutions should be implemented; best practices would include filters that implement *machine learning* and the use of *multi-factor authentication*, with planned responses to *ransomware* and *deepfakes*. Future *phishing* attempts are likely to be become increasingly targeted and immune to these measures, so technological solutions must be supplemented with human-focused policy as well. Our findings strongly suggest both *training* and *testing* are necessary, but that these efforts still will not produce complete protection.

Note

1. DMARC (Domain-based Message Authentication Reporting and Conformance) is an e-mail validation system designed to protect an e-mail domain from being used for e-mail spoofing, phishing scams and other cybercrimes. DMARC leverages the existing e-mail authentication techniques, such as SPF (Sender Policy Framework) and DKIM (Domain Keys Identified Mail).

Acknowledgments

We would like to thank our interview respondents.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Adam Kavon Ghazi-Tehrani http://orcid.org/0000-0001-5750-0901
Henry N. Pontell http://orcid.org/0000-0003-2487-4581

Data availability

Data available upon request.

References

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, *82*(October), 69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005

Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, *29*(3), 706–714. https://doi.org/10.1016/j.chb.2012.12.018

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*(September), 304–312. https://doi.org/10.1016/j.chb.2014.05.046

Barnes, J. (2020, June 16). C.I.A. failed to defend against theft of secrets by insider, report says. *The New York Times*.

Barratt, M. J., Ferris, J. A., & Lenton, S. (2015). Hidden populations, online purposive sampling, and external validity: Taking off the blindfold. *Field Methods*, *27*(1), 3–21. https://doi.org/10.1177/1525822X14526838

Bellaby, R. W. (2018). Going dark: Anonymising technology in cyberspace. *Ethics and Information Technology*, *20*(3), 189–204. https://doi.org/10.1007/s10676-018-9458-4

Birks, M., & Mills, J. (2011). *Grounded theory: A practical guide*. Sage.

Bossler, A., & Holt, T. (2009). On-line activities, guardianship, and malware infection: An examination of Routine Activities Theory. *International Journal of Cyber Criminology (IJCC)*, *3*(1), 974–2891. http://www.cybercrimejournal.com/bosslerholtijcc2009.pdf

Braithwaite, J. (1989). *Crime, shame, and reintegration*. Cambridge University Press.

Brewer, R. (2016). Ransomware attacks: Detection, prevention and cure. *Network Security*, *2016*(9), 5–9. https://doi.org/10.1016/S1353-4858(16)30086-1

Charmaz, K. (2006). *Constructing grounded theory*. Sage Publications.

Clarke, R. V. G., Great Britain, Home Office, & Policing and Reducing Crime Unit. (1999). *Hot products: Understanding, anticipating and reducing demand for stolen goods*. Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate. http://books.google.com/books?id=-iEEAQAAIAAJ

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588. https://doi.org/10.2307/2094589

Cook, D. L., Gurbani, V. K., & Daniluk, M. (2009). Phishwish: A simple and stateless phishing filter. *Security and Communication Networks*, *2*(1), 29–43. https://doi.org/10.1002/sec.45

Corbin, J. M., & Strauss, A. L. (2008). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (3rd ed.). Sage Publications, Inc.

Crawford, M., Khoshgoftaar, T. M., Prusa, J. D., Richter, A. N., & Al Najada, H. (2015). Survey of review spam detection using machine learning techniques. *Journal of Big Data*, *2*(1), 23. https://doi.org/10.1186/s40537-015-0029-9

Crenson, M. A. (1972). *The un-politics of air pollution: A study of non-decisionmaking in the cities*. Johns Hopkins Pr.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed., international student edition). SAGE.

Crocker, A. (2020, June 24). *The Senate's new anti-encryption bill is even worse than EARN IT, and that's saying something*. EFF. https://www.eff.org/deeplinks/2020/06/senates-new-anti-encryption-bill-even-worse-earn-it-and-thats-saying-something

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI conference on human factors in computing systems - CHI '06*, 581. https://doi.org/10.1145/1124772.1124861

Downs, J., Holbook, M., & Cranor, L. (2006). Decision strategies and susceptibility to phishing. *Symposium on usable privacy and security*, 79–90.

Egan, G. (2020). *State of the Phish*. Proofpoint. https://www.proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical

Etikan, I. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1. https://doi.org/10.11648/j.ajtas.20160501.11

Forst, B. (1983). Capital punishment and deterrence: Conflicting evidence? *The Journal of Criminal Law and Criminology (1973-)*, *74*(3), 927. https://doi.org/10.2307/1143139

Glaser, B. G., & Strauss, A. L. (2009). *The discovery of grounded theory: Strategies for qualitative research* (4. paperback printing). Aldine.

Gold, S. (2011). Cracking wireless networks. *Network Security*, *2011*(11), 14–18. https://doi.org/10.1016/S1353-4858(11)70120-9

Gorham, M. (2020). *2019 Internet crime report*. Federal Bureau of Investigation. https://pdf.ic3.gov/2019_IC3Report.pdf

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

Green, A. (2013, January 16). *"Aaron's Law" suggests reforms to computer fraud act (but not enough to have protected Aaron Swartz)*. Forbes. https://www.forbes.com/sites/andygreenberg/2013/01/16/aarons-law-suggests-reforms-to-hacking-acts-but-not-enough-to-have-protected-aaron-swartz/#44845bf66649

Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2018). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*(2), 247–267. https://doi.org/10.1007/s11235-017-0334-z

Harris, E. (2014, April 29). After data breach, target plans to issue more secure chip-and-PIN cards. *The New York Times*. https://www.nytimes.com/2014/04/30/business/after-data-breach-target-replaces-its-head-of-technology.html

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Howell, C. J., Burruss, G. W., Maimon, D., & Sahani, S. (2019). Website defacement and routine activities: Considering the importance of hackers' valuations of potential targets. *Journal of Crime and Justice*, *42*(5), 536–550. https://doi.org/10.1080/0735648X.2019.1691859

Hutchings, A., Smith, R. G., & James, L. (2015). Criminals in the cloud: Crime, security threats, and prevention measures. In R. G. Smith, R.-C.-C. Cheung, & L. Y.-C. Lau (Eds.), *Cybercrime risks and responses: Eastern and Western perspectives* (pp. 146–162). Palgrave Macmillan UK. https://doi.org/10.1057/9781137474162_10

Hutchings, A., & Hayes, H. (2009). Routine Activity Theory and phishing victimisation: Who gets caught in the 'net'? *Current Issues in Criminal Justice*, *20*(3), 433–452. https://doi.org/10.1080/10345329.2009.12035821

Kahan, D. M., & Posner, E. A. (1999). Shaming White-Collar criminals: A proposal for reform of the federal sentencing guidelines. *The Journal of Law and Economics*, *42*(S1), 365–392. https://doi.org/10.1086/467429

Kassner, M. (2015, February 2). Anatomy of the target data breach: Missed opportunities and lessons learned. *ZDNet*. https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

Kennedy, E., & Millard, C. (2016). Data security and multi-factor authentication: Analysis of requirements under EU law and in selected EU Member States. *Computer Law & Security Review*, *32*(1), 91–110. https://doi.org/10.1016/j.clsr.2015.12.004

Kigerl, A. (2012). Routine Activity Theory and the determinants of high cybercrime countries. *Social Science Computer Review*, *30*(4), 470–486. https://doi.org/10.1177/0894439311422689

Krebs, B. (2015, August 7). Tech firm Ubiquiti suffers $46M cyberheist. *Krebs on Security*. https://krebsonsecurity.com/2015/08/tech-firm-ubiquiti-suffers-46m-cyberheist/

Leukfeldt, E. (2014). Phishing for suitable targets in The Netherlands: Routine Activity Theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551–555. https://doi.org/10.1089/cyber.2014.0008

Leukfeldt, E. (2015). Comparing victims of phishing and malware attacks: Unraveling risk factors and possibilities for situational crime prevention. *ArXiv:1506.00769 [Cs]*. http://arxiv.org/abs/1506.00769

Leukfeldt, E., Kleemans, E. R., & Stol, W. P. (2016). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology*, *57*(3). https://doi.org/10.1093/bjc/azw009

Leukfeldt, E., & Yar, M. (2016). Applying Routine Activity Theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Maddocks, S. (2020). 'A deepfake porn plot intended to silence me': Exploring continuities between pornographic and 'political' deep fakes. *Porn Studies*, 1–9. https://doi.org/10.1080/23268743.2020.1757499

Malecki, F. (2019). Best practices for preventing and recovering from a ransomware attack. *Computer Fraud & Security*, *2019*(3), 8–10. https://doi.org/10.1016/S1361-3723(19)30028-4

Mansfield-Devine, S. (2016a). Ransomware: Taking businesses hostage. *Network Security*, *2016*(10), 8–17. https://doi.org/10.1016/S1353-4858(16)30096-4

Mansfield-Devine, S. (2016b). The imitation game: How business email compromise scams are robbing organisations. *Computer Fraud & Security*, *2016*(11), 5–10. https://doi.org/10.1016/S1361-3723(16)30089-6

Morrison, D. E., & Firmstone, J. (2000). The social function of trust and implications for e-commerce. *International Journal of Advertising*, *19*(5), 599–623. https://doi.org/10.1080/02650487.2000.11104826

Murphy, K., & Harris, N. (2007). Shaming, shame and recidivism: A test of reintegrative shaming theory in the White-Collar crime context. *British Journal of Criminology*, *47*(6), 900–917. https://doi.org/10.1093/bjc/azm037

Nasralla, S. (2016, May 25). *Austria's FACC, hit by cyber fraud, fires CEO*. Reuters. https://www.reuters.com/article/us-facc-ceo/austrias-facc-hit-by-cyber-fraud-fires-ceo-idUSKCN0YG0ZF

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773–793. https://www.cybercrimejournal.com/ngo2011ijcc.pdf

O'Neill, P. H. (2020, January 2). Ransomware may have cost the US more than $7.5 billion in 2019. *MIT Technology Review*. https://www.technologyreview.com/f/615002/ransomware-may-have-cost-the-us-more-than-75-billion-in-2019/

Ohlheiser, A. (2016, May 24). The shockingly simple way the nude photos of 'Celebgate' were stolen. *The Washington Post*. https://www.washingtonpost.com/news/the-intersect/wp/2016/03/16/the-shockingly-simple-way-the-nude-photos-of-celebgate-were-stolen/

Öhman, C. (2020). Introducing the pervert's dilemma: A contribution to the critique of deepfake pornography. *Ethics and Information Technology*, *22*(2), 133–140. https://doi.org/10.1007/s10676-019-09522-1

Pantserev, K. A. (2020). The Malicious use of AI-based deepfake technology as the new threat to psychological security and political stability. In H. Jahankhani, S. Kendzierskyj, N. Chelvachandran, & J. Ibarra (Eds.), *Cyber defence in the age of AI, smart societies and augmented humanity* (pp. 37–55). Springer International Publishing. https://doi.org/10.1007/978-3-030-35746-7_3

Parmar, B. (2012). Protecting against spear-phishing. *Computer Fraud & Security*, *2012*(1), 8–11. https://doi.org/10.1016/S1361-3723(12)70007-6

Pontell, H. N. (1982). System capacity and criminal justice: Theoretical and substantive considerations. In H. E. Pepinsky (Ed.), *Rethinking criminology* (pp. 131–143). Sage Publications.

Pontell, H. N., Calavita, K., & Tillman, R. (1994). Corporate crime and criminal justice system capacity: Government response to financial institution fraud. *Justice Quarterly*, *11*(3), 383–410. https://doi.org/10.1080/07418829400092321

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. https://doi.org/10.1177/0022427810365903

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–Routine Activities Theory to cyberstalking victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169. https://doi.org/10.1177/0093854811421448

Richmond, R. (2011, April 2). The RSA hack: How they did it. *The New York Times*. https://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/

Rizzo, J. (2012, August 2). *Cybersecurity bill fails in Senate*. CNN. https://www.cnn.com/2012/08/02/politics/cybersecurity-act/index.html

Romo, V. (2019, March 25). *Man pleads guilty to phishing scheme that fleeced Facebook, Google of $100 Million*. NPR. https://www.npr.org/2019/03/25/706715377/man-pleads-guilty-to-phishing-scheme-that-fleeced-facebook-google-of-100-million

Rosoff, S. M., Pontell, H. N., & Tillman, R. (2014). *Profit without honor: White-collar crime and the looting of America* (6th ed.). Pearson.

Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. *Expert Systems with Applications*, *117*(March), 345–357. https://doi.org/10.1016/j.eswa.2018.09.029

Schneider, O. (2016, January 19). Belgian bank Crelan hit by a 70 million Eur fraud. *The Brussels Times*. https://www.brusselstimes.com/news/belgium-all-news/36335/belgian-bank-crelan-hit-by-a-70-million-eur-fraud/

Scholz, J. T. (1997). Enforcement policy and corporate misconduct: The changing perspective of deterrence theory. *Law and Contemporary Problems*, *60*(3), 253. https://doi.org/10.2307/1192014

Smith, M. (2013, May 12). U.S. government is "biggest buyer" of zero-day vulnerabilities, report claims. *CSO Online*. https://www.csoonline.com/article/2224620/u-s–government-is–biggest-buyer–of-zero-day-vulnerabilities–report-claims.html

Stake, R. E. (2010). *Qualitative research: Studying how things work*. Guilford Press.

Stalans, L. J., & Donner, C. M. (2018). Explaining why cybercrime occurs: Criminological and psychological theories. In H. Jahankhani (Ed.), *Cyber Criminology* (pp. 25–45). Springer International Publishing. https://doi.org/10.1007/978-3-319-97181-0_2

Stembert, N., Padmos, A., Bargh, M. S., Choenni, S., & Jansen, F. (2015). A study of preventing email (spear) phishing by enabling human intelligence. *2015 European intelligence and security informatics conference*, 113–120. https://doi.org/10.1109/EISIC.2015.38
Stupp, C. (2019, August 30). Fraudsters used AI to Mimic CEO's voice in unusual cybercrime case. *The Wall Street Journal*. https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402
Sun, J. C.-Y., Yu, S.-J., Lin, S. S. J., & Tseng, -S.-S. (2016). The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference. *Computers in Human Behavior*, *59*(June) 249–257. https://doi.org/10.1016/j.chb.2016.02.004
Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., Markov, Y., Comanescu, O., Eranti, V., Moscicki, A., Margolis, D., Paxson, V., & Bursztein, E. (2017). Data breaches, phishing, or malware?: Understanding the risks of stolen credentials. *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, 1421–1434. https://doi.org/10.1145/3133956.3134067
Urquhart, C. (2013). *Grounded theory for qualitative research: A practical guide*. SAGE.
Van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology*, *8*(2), 115–127. https://doi.org/10.1177/1477370810393156
Van Wilsem, J. (2013). "Bought it, but never got it" assessing risk factors for online consumer fraud victimization. *European Sociological Review*, *29*(2), 168–178. https://doi.org/10.1093/esr/jcr053
Verizon. (2019). *2018 data breach investigations report*. https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf
Weimann, G. (2016). Going dark: Terrorism on the Dark Web. *Studies in Conflict & Terrorism*, *39*(3), 195–206. https://doi.org/10.1080/1057610X.2015.1119546
Whitaker, A., & Newman, D. P. (2006). *Penetration testing and network defense*. Cisco Press.
Wilhelm, T. (2013). *Professional penetration testing* (2nd ed.). Syngress, an imprint of Elsevier.
Wojewidka, J. (2020). The deepfake threat to face biometrics. *Biometric Technology Today*, *2020*(2), 5–7. https://doi.org/10.1016/S0969-4765(20)30023-0
Wortley, R., & Tilley, N. (2014). Theories for situational and environmental crime prevention. In G. Bruinsma & D. Weisburd (Eds.), *Encyclopedia of criminology and criminal justice* (pp. 5164–5173). Springer New York. https://doi.org/10.1007/978-1-4614-5690-2_548
Wu, T. (2013, March 18). Fixing the worst law in technology. *The New Yorker*. https://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology
Yang, W., Chen, J., Xiong, A., Proctor, R. W., & Li, N. (2015). Effectiveness of a phishing warning in field settings. *Proceedings of the 2015 symposium and bootcamp on the science of security - HotSoS '15*, 1–2. https://doi.org/10.1145/2746194.2746208
Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407–427. https://doi.org/10.1177/147737080556056
Zetter, K. (2014, November 17). U.S. gov insists it doesn't Stockpile zero-day exploits to hack enemies. *WIRED*. https://www.wired.com/2014/11/michael-daniel-no-zero-day-stockpile/

Appendix. Interview Schedule

RQ1: What factors allow *phishing* to exist as a long-term, successful crime type?
RQ1A: How is *phishing* different now than 5 years ago? 10 years? 20 years?
RQ1B: You have mentioned (MOTIVATION, COSTS, RISKS, REWARDS, OFFENDER, VICTIM) but what about (ADDRESS ANY MISSING)?
RQ1C: Do you know of any exemplary cases of *phishing* (noteworthy targets, methods, or offenders)?

RQ2: What *technological* solutions are viable now; and in the future?
RQ2A: Conversely, are any *technological* problems on the horizon?
RQ2B: Which solutions do not work and why?

RQ2C: How should *technological* solutions be implemented (personal choice, corporate responsibility, or via government regulation)?

RQ3: What *human-focused* prevention strategies are viable now; and in the future?
RQ3A: Conversely, are any *human-focused* problems on the horizon?
RQ3B: Which solutions do not work and why?
RQ3C: How should *human-focused* prevention strategies be implemented (personal choice, corporate responsibility, or via government regulation)?