



Prevention and mitigation measures against phishing emails: a sequential schema model

Yumi E. Suzuki¹ · Sergio A. Salinas Monroy²

Accepted: 14 September 2021 / Published online: 28 September 2021
© The Author(s), under exclusive licence to Springer Nature Limited 2021

Abstract

Phishing emails have permeated our digital communication, taking advantage of vulnerabilities that the information technology system poses to users. Given the potential for further cybersecurity incidents, theft of personally identifiable information, and damage to organizations' assets, cybersecurity professionals have implemented various mitigation practices to combat phishing emails. This paper categorizes current mitigation practices in relation to a sequential schema adopted from the situational crime prevention approach, so as to enable a more organized and strategic assessment of human and environmental vulnerabilities. Our model could be useful for cybersecurity professionals to further advance mitigation measures as an incident progresses and for criminologists and other academic researchers to reduce the severity of subsequent criminal incidents.

Keywords Phishing email · Mitigation · Cybersecurity · Personally identifiable information

Introduction

As early as March 9, 2020, the U.S. Secret Service (2020) was releasing statements alerting the public about well-crafted phishing emails related to the coronavirus. Opportunistic criminals have continued to engage in email scams, aimed especially at healthcare and pharmaceutical providers, involving information and supplies related to the coronavirus (FinCEN 2020). Although phishing emails have existed since the advent of the email communication system, significant increases

✉ Yumi E. Suzuki
Yumi.suzuki@wichita.edu

Sergio A. Salinas Monroy
Sergio.salinasmonroy@wichita.edu

¹ School of Criminal Justice, Wichita State University, 1845 Fairmount St., Wichita, KS 67260-0135, USA

² School of Computing, Wichita State University, Wichita, USA



in phishing campaigns amid the pandemic, observed by FinCEN and other federal agencies, such as the U.S. Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA), have indicated the need for strategic vigilance at the individual and organizational levels. Individuals are gatekeepers to personally identifiable information (PII)¹ and potentially sensitive data that could impact an organization's assets. A report by Proofpoint (2021a) documents how successful phishing attacks in 2020 resulted in the loss of data, credential and account compromise, ransomware infection, and other malware infections.

The FBI's Internet Crime Complaint Center defines phishing as "the use of unsolicited email...purportedly from a legitimate company requesting personal, financial, and/or login credentials" (FBI 2021a, p. 28). As of February 23, 2020, 23 U.S. states and Guam had laws prohibiting phishing, whereas the remaining states address this crime under the categories of computer crime, fraudulent or deceptive practices, or identity theft (National Conference of State Legislatures 2020). Phishing is the most frequently reported internet crime to the FBI (FBI 2021a), and phishing attacks are rising globally (Oest et al. 2018). Webmail and software-as-a-service users (31.4%) and financial institutions (19.2%) were the top two major targets during the third quarter of 2020 (Anti-Phishing Working Group 2020), and the resulting monetary losses suffered by businesses and consumers are growing (FBI 2021a). Phishing emails were the most common type of breach, and they involved organized groups in over half of all cases (Verizon 2020). Phishing emails targeting specific individuals in an organization can result in business email compromise (BEC) that ends with significant financial losses (Better Business Bureau [BBB] 2019; FBI 2021a).

Given the wide-ranging and severe threats that phishing emails pose to multiple sectors of organizations, cybersecurity professionals are at the forefront of the fight against persistent phishers and their evolving methods. Meanwhile, criminologists with expertise in cybercrime have made modest advancements in the conceptualization and application of theoretical frameworks suitable for addressing phishing emails. Cybercrime is a reasonably new addition to the field of criminology/criminal justice, and it is an inherently international and interdisciplinary field of study (Payne and Hadzhidimova 2020). Many of the prevention and mitigation practices that cybersecurity professionals have proposed or adopted to thwart other types of attacks are often based on the situational crime prevention (SCP) approach (Willison and Siponen 2009) or compatible with it. By adopting and adjusting the crime script model from SCP, this paper configures techniques drawn from current cybersecurity practices to prevent and mitigate phishing attacks.

Increased investments in cybersecurity training by many organizations reveal the critical role of human vulnerabilities for which the organization's infrastructure alone cannot compensate (Steves et al. 2020). Although organizations can purchase anti-phishing software or phishing awareness training from various vendors, gaining a systematic understanding of phishing approaches based on SCP may complement

¹ Throughout this paper, PII refers to any information identified with or identifiable as relating to a particular individual, such as credentials for online accounts, medical or financial information, IP addresses, phone numbers, and facial images to unlock smartphones (Nanduru 2021)



existing anti-phishing mechanisms by revealing both human and environmental (i.e., organizational) vulnerabilities.

Beginning with the broader impact of phishing emails, we describe the current state of phishing email defenses. We then discuss in detail the proposed model and its application for combating phishing attacks, with descriptions of prevention and mitigation measures.

The broader impact of phishing emails

According to HP-Bromium (2020), most malware was delivered by email during the fourth quarter of 2020. Malware can be disguised as an attachment or a URL in phishing emails, and malware payloads may include remote access Trojans, downloaders, keyloggers (Proofpoint 2021a), and ransomware (Greenman et al. 2021). Kratikal (2020), a network security company, observed that almost all phishing emails (97%) received by their customers during 2020 contained ransomware. A recent alert from the FBI (2021b) sent to cybersecurity professionals and system administrators highlighted an increase in ransomware attacks on educational institutions, initiated by compromising Remote Desktop Protocol (RDP) credentials or phishing emails. Over one-quarter of organizations infected with ransomware in 2020 paid the ransom; of these, 60% regained access to data or systems after the first payment, whereas 32% of them had to pay an additional ransom (Proofpoint 2021a).

The deployment of ransomware in industrial control systems (ICS), such as manufacturing plants or the power grid, has grown steadily in incidence and sophistication over the last few years. Brubaker et al (2020) reported what appeared to be the first malware designed for an ICS and delivered through a phishing email in 2020. Other security companies have also noted this trend (FortiNet Guard Labs 2020). Ransomware deployed via malware in phishing emails that targets ICS is of particular concern due to the potentially catastrophic consequences for critical infrastructure.

For example, when the Colonial Pipeline Company announced its operational halt due to a ransomware attack on May 8, 2021, gasoline supplies throughout the East Coast were disrupted (Congressional Research Service 2021), bringing cybersecurity of ICS to the attention of federal agencies and the U.S. Congress. Although the ransomware attack at Colonial Pipeline appears to have been deployed to its networks via a compromised password (Fung and Sands 2021), the culprit in the attack, DarkSide, has previously used phishing emails and RDP to infiltrate targeted systems (FBI and CISA 2021). In response to this incident, on May 27, 2021, the Transportation Security Administration issued a directive to critical pipeline owners and operators regarding specific cybersecurity requirements (DHS 2021a), followed by an additional directive requiring measures against ransomware attacks and other cybersecurity issues (DHS 2021b). Because of a series of high-profile ransomware attacks in addition to the one that impacted Colonial Pipeline, the U.S. Department of Justice (DOJ) and the DHS announced on July 15, 2021, the launch of a one-stop ransomware resource website (DOJ 2021). Furthermore, CISA and the FBI released



a joint advisory on July 20, 2021, alerting ICS stakeholders regarding detailed information on the past intrusion campaigns targeting ICS (CISA 2021a).

Another common consequence of phishing email attacks is identity theft (Finklea 2014). In addition to Verizon's data breach report (2020), which showed that organized criminals were involved in more than half of the breaches, a myriad of federal cases has corroborated the nexus between identity theft and organized crime (e.g., DOJ 2014, 2017; FBI, n.d.). The FBI (2006) has indicated explicitly that its identity theft investigations target organized groups and criminal enterprises to maximize efficient use of resources. The allocation of law enforcement resources and efforts to the identity theft–organized crime nexus may be timely, given the increasing trend of identity theft as reported by the Federal Trade Commission (2021) and the resurgence of schemes taking advantage of the pandemic, such as government benefit frauds.

Additionally, experts in identity crime services have increasingly recognized this nexus (Green et al. 2020). Collaboration among law enforcement, cybersecurity professionals, academic researchers, and victim service providers may offer a more comprehensive picture of the role of phishing emails in identity theft, opportunities to assess existing investigative tools and technologies, and strategies for protecting PII at both individual and organizational levels. Button and Cross (2017) pointed out that fraud and scams have not been a high priority for law enforcement, thereby perhaps generating misconceptions about the severity of these crimes and their actual impact on victims. They also lamented a lack of literature addressing fraud prevention measures. Since phishers typically have almost nine hours between the first victim's visit to a fraudulent website and anti-phishing mechanisms' detection of their phishing site as malicious, and an additional 12 hours until the last unsuspecting victim visits the malicious site (Oest et al. 2020b), strategic efforts to minimize the potential damage are essential for both individuals and organizations. In collaboration with concerned professionals, academic researchers could conduct innovative studies on identity theft or resulting fraud to advance knowledge and best practices among the professional community and raise awareness about potential harms to the public.

Current understanding of phishing attacks

Current phishing attack prevention techniques focus mainly on preventing phishing emails from reaching the users' inboxes and on discouraging users from accessing phishing websites. These approaches can be classified into email filters, blocking of phishing websites, and user training.

Email filters to prevent phishing emails have been extensively studied and are widely used by email service providers (Karim et al. 2019). Email filters are software applications that run on email servers. Their objective is to inspect email messages addressed to users within an organization and to classify them as legitimate or malicious messages. Legitimate messages are forwarded to the addressed users; malicious messages can be deleted, sent to the addressed users' spam folder, or stored by the email server for further analysis. Email filters prevent users from clicking on



potentially malicious URLs in the email messages or engaging in email conversations with the attacker by keeping those users from ever receiving the message.

Email filters use multiple strategies to classify email messages (El Aassal et al. 2020). They initially attempt to determine whether the email message was sent from a legitimate source by checking the sender's email address against a phishing or spam blacklist. The email filter also verifies that the public key from the sender's email server matches its IP address and domain name. It does so by using the Sender Policy Framework (SPF) and DomainKeys Identified Mails (DKIM) protocols.

After establishing the email sender's legitimacy, the email filter then inspects URLs within the body of the email message. The filter first checks the URLs against widely used blacklists maintained by the Internet community and security companies (Oest et al. 2020a). If the URL is on the blacklist, the email is classified as malicious. If it does not appear on any blacklist, the filter can proceed to run one of various phishing URL detectors. These detectors employ heuristics and artificial intelligence to determine whether the URL's features are consistent with those of previously identified phishing URLs.

Although the email filtering techniques described above successfully classify many phishing emails as malicious messages, attackers can still evade the filters by carefully crafting their messages (Hu and Wang 2018). For example, attackers may use legitimate email accounts from various email service providers to bypass the sender legitimacy check. They can also evade the URL check by hosting their phishing websites on previously compromised domains of legitimate organizations. Furthermore, they may send phishing emails that contain no URLs at all, hoping instead to engage victims in correspondence and persuade them to act on behalf of the attacker. Lastly, all email filters have a certain false-negative rate that results in some malicious messages being classified as legitimate.

A second way for system administrators to protect their users from phishing attacks is by blocking the domains known to host phishing websites. In this approach, users are prevented from accessing any domain that appears on one of the widely used blacklists. Even if a malicious email with a URL pointing to a phishing website bypasses the email filter, users are restrained from opening the website, thereby protecting them from falling victim to a phishing scam.

To prevent users from accessing a domain, system administrators can configure their firewalls to block all outgoing connections to the domain's IP address or the domain. They can also configure their domain name system (DNS), which translates URLs to IP addresses for users, to return a default IP address when a user requests access to a blacklisted domain.

The third technique employed to prevent phishing attacks is to educate users about phishing attacks, either by providing reminders of potential phishing attempts in incoming emails or by offering on-site or online training. System administrators can install software that displays alert messages on emails sent from outside the organization (Thompson et al. 2019). Such alerts have demonstrated some effectiveness (Xiong et al. 2017). Reminders briefly explaining what phishing is to users have also been described as a promising practice (Reinheimer et al. 2020).

Direct training through workshops is another way to educate users about the danger of phishing and how to spot examples. As users become aware of phishing



emails and how they work, they are more likely to notice them in their inboxes. This approach has had substantial success, but research has shown that a small proportion of users remain vulnerable to phishing scams even after training (Singh et al. 2019).

Although the above techniques constitute an essential first line of defense against phishing attacks, they ignore the subsequent steps of a phishing attack, that is, what happens after a criminal manages to use phishing emails and websites to steal users' credentials and PII. Once attackers have access to the organization's networks via the stolen credentials, they perform actions that can cause considerable harm to victims, including intellectual property theft, access to bank accounts using stolen personal information, and installing ransomware.

In the following discussion, we adapt some of the tools of SCP to highlight how some cybersecurity best practices can be used to protect organizations against all steps of phishing attacks.

Applying the situational crime prevention approach to phishing emails

The situational crime prevention approach is rooted primarily in the rational choice perspective of an individual's assessment for crime commission based on perceived rewards and risks (Clarke 1983; Cornish and Clarke 1987), as well as in routine activity approach of three elements of a direct-contact predatory crime (Cohen and Felson 1979). Specifically, SCP takes into consideration the offender's decision in weighing the costs and benefits of offending as well as the convergence of a motivated offender, a suitable target, and the absence of a capable guardian as necessary prerequisites for a crime to occur (Bossler 2020). SCP yields crime prevention measures targeting a specific type of crime by systematically manipulating the environment "to reduce the opportunities for crime and increase its risks as perceived by a wide range of offenders" (Clarke 1983, p. 225). Thus, it seeks to decrease the prospects of crime by limiting the opportunities to commit crime (or situational components of crime) and impacting perceptions and decisions about offending (Clarke 1983; Ekblom 2017; Smith and Clarke 2012). These can be done by physically blocking or increasing the effort in obtaining crime opportunities, by increasing the actual (or perception of the) risks of crime, and by limiting the rewards associated with the crime. SCP also can, in some situations, reduce the factors making a criminal decision more likely and remind potential offenders about the rules of behavior (Cornish and Clarke 2003). Rather than focusing on the criminal justice system to sanction illegal behavior, SCP relies on organizations to reduce crime opportunities by making their environments less conducive to committing crimes (Clarke 1997).

The original eight-technique classification scheme of SCP, published in 1980 (Hough et al. 1980), offered potential mechanisms and techniques applicable in certain situations (Smith and Clarke 2012). Later, a 12-technique classification scheme focusing on the prevention concepts of effort, risk, and reward was introduced (Clarke 1992), followed by a 16-technique scheme with a new classification category of guilt or shame (Clarke and Homel 1997). In response to Wortley's (2001) critique of SCP and his proposal of situational precipitation strategies with four control



mechanisms (related to prompts, pressures, permissibility, and provocations), Cornish and Clarke (2003) presented a revised and updated classification scheme, which included five techniques, each of which is categorized under five prevention mechanisms. Acknowledging “the importance of addressing the interaction between the offender and his or her environment” and “the general value of situational crime prevention as a way of controlling crime by trying to understand and manage aspects of this interaction” (Cornish and Clarke 2003, p. 50), the latest classification scheme incorporates reducing provocations and removing excuses as additional prevention mechanisms to the existing three mechanisms from the two previous versions (i.e., Clarke 1992; Clarke and Homel 1997), namely increasing the effort, increasing the risks, and reducing the rewards for committing a crime.

Although limited in scope and application, SCP has been utilized to reduce the risk of various types of cybercrimes. Hartel et al (2011) demonstrated that SCP techniques apply to crimes occurring in cyberspace just as to more traditional crimes offline. SCP has been used to address information security (Hinduja and Kooi 2013; Willison and Backhouse 2006; Willison and Siponen 2009), cybersecurity (Back and LaPrade 2020), cyber frauds and scams (Button and Cross 2017), and cyberstalking (Reyns 2010).

Unlike other forms of cybercrime, in which motives are known and victim types are consistent, phishers are likely to have varying goals, motivations, and victim types.² For example, a phisher may seek to steal PII from a government agency only to subsequently steal highly sensitive information. Similarly, a phisher may enter an individual victim’s system to steal credentials, but may go further by demanding a ransom in exchange for releasing the victim’s system and data. Thus, our model purposely covers phishing emails regardless of perceived motives, goals, or victim types, as a phishing email is both a specific crime and a mechanism by which to commit additional crimes. Furthermore, phishers’ true motives may be unknown and their goals may change as they swim through the target systems. However, the utility of two aspects of the SCP approach, bounded rationality and crime scripts, may provide potentially sustainable applications to the phishing email defense.

Bounded rationality, developed by Simon (1955, 1957), considers “the cognitive limitations of [goal-oriented] decision makers in attempting to achieve those goals” (Jones 1999, p. 299). In the case of phishers, these limitations may include time, ability or skills, knowledge, and resources available to accomplish varying goals of phishing attacks. Parker (1998) proposed that key characteristics of cybercriminals include skills, knowledge, resources, authority, and motives (SKRAM).

² Both monetary motives and the pursuit of data theft, including intellectual property and other espionage purposes, have been reported in 2020 (FireEye Mandiant Services 2021). For example, a cyberespionage group, Iron Liberty, has used phishing emails to access ICS (Secureworks 2019). A more well-known example of varying motives of phishers was observed in the 2016 phishing of an email account owned by John Podesta, who was the campaign chairman for Hillary Clinton (Gupta et al. 2018), so as to influence a U.S. presidential election. As these examples illustrate, phishers target individual victims, businesses, and organizations (FBI 2021a) as well as governments (HP-Bronium 2020). The preferred method of infiltrating the target systems via phishing emails appears consistent, as indicated by a recent threat report (Proofpoint 2021b)



Understanding criminals' exhibited skills used to penetrate the system, their knowledge of the phishing ecosystem from the onset of attacks to the end of the phishing lifecycle, the resources they use to launch phishing attacks, and in some cases their possession of a privileged or authorized access (usually obtained via the physical theft of credentials or by abusing rights to access certain applications or files) may help devise specific mitigation measures as phishers make procedural decisions with bounded rationality.

Another critical component of SCP's evolving applicability to versatile crimes is the use of crime scripts. A crime script, or an event schema, "organizes our knowledge about how to understand and enact commonplace behavioral processes or routines" (Cornish 1994, p. 158). Specifically, a script helps cybersecurity professionals to examine a sequence of events at each stage of crime commission and evaluate suitable safeguards (Willison and Backhouse 2006; Willison and Siponen 2009). Detailed prevention or mitigation measures can thus be identified and then implemented at each stage to halt the progression of criminal events.

With these two advantages of SCP in mind, we have identified prevention and mitigation measures to counter phishing attacks. Consistent with the purpose of SCP, our list of these measures should be viewed as a worksheet for implementing and improving phishing email prevention/mitigation practice and policy in an organization, not as an exhaustive set of options. Thus, our model should not replace the cybersecurity framework of practices specified by the U.S. National Institute of Standards and Technology (NIST 2018)³ or other organizations, such as the International Organization for Standardization. Rather, our model is specific to one particular security issue (i.e., phishing emails) and can complement the current behavior-based frameworks⁴ to achieve an increased awareness of situational vulnerabilities. As phishers' tactics evolve, our prevention and mitigation measures must do so as well.

Prevention/mitigation points and measures

The first and second columns of Table 1 present a crime script in which the scene function (first column) shows a generic progression of a crime (adopted from Cornish 1994), followed by the script action (second column) that demonstrates a phishing

³ Our model shares some similarities with the NIST framework of identify, protect, detect, respond, and recover. For example, under the protect category, implementing access control and awareness training is suggested; both of these measures are included in our model. Although the NIST cybersecurity framework was originally developed for critical infrastructure, it can be implemented by other organizations in any sector that rely on IT, ICS, and the IoT (NIST 2018). NIST also makes available the Computer Security Incident Handling Guide (Cichonski et al. 2012).

⁴ In addition to frameworks proposed by NIST and other organizations, the MITRE ATT&CK cyber adversary behavioral model is widely used by cybersecurity professionals and organizations, including CISA. This model includes attack tactics, goals, and techniques to accomplish tactics in phases (Strom et al. 2020). For example, attackers may use phishing as initial access, followed by command and scripting interpreter as execution, access token manipulation as privilege escalation, and two-factor authentication interception as credential access (see Strom et al. 2020, p. 6 for the matrix of techniques).



attack sequence. The third column, situational control, has a broadly defined objective that corresponds to a tactic to accomplish the objective. The last column details prevention or mitigation measures matching situational control's objectives and tactics. At any point in the script action, the element of the phisher's bounded rationality may become known to cybersecurity professionals. For example, high-tech phishers may have the skills, knowledge, and resources to acquire the phishing infrastructure needed to launch wide-scale attacks, which are commonly initiated by launching deceptive websites, sending emails to potential victims, and downloading the stolen information (Oest et al. 2020b). System administrators, in turn, could strengthen network security and guardianship provided by the organization. Similarly, the process of phishers gaining authorized access to specific files or programs may be reverse-engineered to reveal a potential source of a security breach. Knowledge of what constraints phishers are willing or unwilling to overcome can be valuable information facilitating an assessment of the durability of the organization's existing cybersecurity. Below, we further explain mitigation measures that correspond to the progression of phishing attacks and the situational objective of each measure.

Situational control objective 1: increase the effort of a successful phishing attack

When phishers scour online sources for emails or obtain compromised emails, a phishing kit can be used to launch phishing attacks. With the requisite phishing infrastructure in place, massive phishing emails are on the way with a simple click. Ways to counter phishers' efforts to gain access to PII and the organization's sensitive information include limiting one's presence in the publicly available data that could be used for open-source intelligence (OSINT), restricting access by users, and protecting access for users.

Limit presence in OSINT

One of the key measures taken by individuals or organizations is to limit publicly available information, thereby reducing the chance that phishers will acquire contact information to launch phishing attacks or conduct personalized phishing scams (BBB 2019). OSINT, therefore, can be used for or against phishing. For example, phishers may collect information from public and social networking sites to exploit potential victims. The United Kingdom's National Cyber Security Centre (NCSC 2018) recommends examining the information available on the organization's website and social media. System administrators may assess the level of publicly available organizational information, particularly contact information, to determine what is truly necessary. Likewise, system administrators may consider blocking subscriptions to unknown websites to reduce presence in OSINT.

Restricted access by users

Potential victims can safeguard themselves against phishers by restricting their publicly available information, such as personal or business email addresses or any



Table 1 Mitigation points for phishing attacks

Scene function	Situational control		Mitigation measures
	Script action	Tactic	
Preparation	Scour online for emails Obtain email addresses	(1) Increase the effort of a successful phishing attack.	Limit personal info available to the public
Entry	Set up phishing infrastructure Trigger phishing infrastructure to send emails	Restricted access by users	Block subscription to unknown websites Avoid publishing personal or business email addresses online Avoid using business emails for personal subscriptions
Precondition	Wait for email response Wait for URL clicks Wait for attachment to open	(2) Clarify users' responsibility	Email filter Automatic spam folder Honey accounts Disable compromised credentials IT training Promote organizational email policy Develop credential disclosure policy Award programs for good email practice
Instrumental pre-condition Instrumental initiation	Collect credentials Enter target network Locate PII	(3) Increase the probability of detecting a phishing attack	Banner alerting potential scams Banner alerting emails from outside organization Flag suspicious URLs in emails Display sender's true email address Display "reply to" Email reply tracking IP-based monitoring Monitor email exchanges and login attempts
		User authentication	Domain verification Strong passwords MF authentication



Table 1 (continued)

Scene function	Script action	Situational control		Mitigation measures
		Objective	Tactic	
Instrumental actualization	Access PII	(4) Limit phishers' ability to find sensitive information	Access control	Privileged access Multiple-person sign off on access to data Limited access to users in local network or VPN
Doing	Extract PII		Network security	Network segregation Firewalls Intrusion detection/prevention systems Data encryption Data backup Automatic OS and software updates
Post-condition	Exit the system	(5) Discourage similar attacks	Database security	No public disclosure of exploited vulnerabilities VPN access to IT
Exit	Close remote connection			



other information that should not be in phishers' hands. Avoiding the use of business emails for private correspondence can also protect against unwanted access. Subscribing to online services using business emails may potentially invite phishers into the organization's system.

Protected access for users

Other measures to increase the effort of a successful phishing attack include filtering emails and utilizing an automatic spam folder (NCSC 2018), which most email service providers offer as a default setting. The accuracy of filtering emails may vary; however, content-based filtering featuring 27 items extracted from emails resulted in successful phishing rates of less than 1% (Bergholz et al. 2010). Compromised credentials should immediately be disabled to mitigate further damage.

System administrators can create so-called honey email accounts at the organizational level to detect phishers and deflect them away from legitimate email accounts. Honey email accounts are intentionally designed to allow attackers to compromise their credentials (Akiyama et al. 2018; Gajek and Sadeghi 2007; Lazarov et al. 2016; Peng et al. 2019). System administrators can fill the honey accounts with seemingly real email traffic to lure phishers into spending an excessive amount of time looking for valuable information. By wasting the phisher's time, honey accounts attempt to reduce their time spent on legitimate accounts.

Situational control objective 2: clarify the user's responsibility

While phishers wait for email responses, URL clicks, or attachments to open, users can be the best defense against further attacks by being vigilant against phishers' tactics. Users may appreciate having situational controls to assist their guardianship, allowing them to be more aware of their role in, and their responsibility for, detecting and minimizing the impact of phishing emails.

Promote acceptable behavior

Among over 2,500 manufacturers and other businesses surveyed, 42% indicated that they did not have or were not sure if they had policies and procedures in place to protect their data and intellectual property (Travelers Risk Control 2016). If they do not already offer it, organizations may consider requiring regular information technology (IT) training that includes awareness of phishing schemes and encourages compliance with email and credential disclosure policies. Reinheimer et al (2020) reported that security awareness training yielded successful identification of phishing and legitimate emails even four months after the training.

In addition to regular training, organizations may consider offering award programs for good email practice. For example, a top employee with no record of phishing compromise and the greatest number of phishing emails reported to the IT team may be given priority parking for a month or some other prized privileges.



Awareness/situational reminders

Equally crucial to promoting acceptable behavior among users are situational reminders of potential phishing attempts (NCSC 2018). Banner alerts for potential scams or emails outside organizations may become more frequent practice than in the previous decade. Flagging suspicious URLs in emails can further alert the users to the sender's likely nefarious intent, thus dissuading them from attempting to access the URLs. Users may also be reminded of the importance of examining the sender's valid email address and the "reply to" field to see if any discrepancy exists, which could be a sign of phishing.

Situational control objective 3: increase the probability of detecting a phishing attack

As phishers gain access to credentials and enter the organization's network to locate PII, organizations that provide specific guardianship and user authentication via IT mechanisms may be in a better position to offer a strong defense against further damage. In this sense, system administrators are in the optimal position to devise suitable mechanisms to detect any phishing attempts.

Better guardianship

Organizations can offer better guardianship by tracking email replies and monitoring the IP addresses involved. Many phishers fill the "from" field in their emails with a legitimate-looking address.⁵ However, they often do not control the address listed in the "from" field. To receive the replies from their victims, phishers fill the "reply to" field with an address that they control. By checking for discrepancies between the "from" and "reply to" addresses, system administrators can detect phishing emails.

In this context, we must note that some legitimate emails may have different addresses in the "from" and "reply to" fields. For example, when a personal assistant sends emails on behalf of her client, an additional method of evaluation is needed to determine whether an email is legitimate. The IP address used by users to access their email accounts is roughly composed of two parts; the first part identifies the Internet service provider (ISP), and the second part identifies the user within the ISP. Although the part of the IP address that identifies the user changes continually, the part that identifies the ISP remains constant. Since users often employ the same set of ISPs to access their accounts (e.g., their home ISP, their mobile ISP, and their work ISP), by monitoring the ISPs that people use to login to their email accounts,

⁵ The CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing) Act of 2003 stipulates a working return email address and a way to opt out of receiving future messages from commercial emailers (Rustad 2019). Providing false and fraudulent email addresses, domain names, or IP addresses can be used by the government or any service providers (Rustad 2019) to lodge a claim against commercial phishers under the CAN-SPAM Act, but not against phishers without legitimate affiliations with commercial entities.



it is possible to identify suspicious logins from different ISPs that may indicate that a remote attacker has compromised an account. Consequently, ISPs can maintain a regular update on IP address blacklisting, such as a DNS-based Blackhole List (DNSBL) (Bhadane and Mane 2017; Gupta et al. 2018).

In addition to monitoring suspicious email exchanges and logins for potential phishing attempts, system administrators can also attempt to identify phishing emails by verifying the signature of the email provider who sent them. The CISA (n.d.) suggests SPF and DKIM in detecting unauthorized emails. SPF enables the recipient to know which mail servers are used from the sender's domain, which in turn shows the DNS "which servers are allowed to send email on behalf of a domain" (Bhadane and Mane 2017, p. 21).

When a legitimate email provider implements DKIM, it signs outgoing emails with its private key, which is a secret value that only the email provider knows. The email provider receiving the signed email message can use standard cryptographic techniques to verify the signature's authenticity. Phishing emails that spoof the "from" address with the address of a provider with DKIM can be easily detected with this technique. An attacker could conceivably set up an email server with DKIM for the sole purpose of sending phishing emails; however, such servers are eventually added to a blacklist that the system administrator should keep up to date. Additionally, CISA (n.d.) has pointed out that DMARC (Domain-based Message Authentication, Reporting & Conformance) "provides the strongest protection against spoofed email, ensuring that unauthenticated messages are rejected at the mail server" (p. 2) if the DMARC reject policy is in place.

User authentication

As the major line of defense, user authentication assigns an identifier, such as a login name, and verifies the user through an authentication process, which is typically accomplished by associating the user with passwords (Stallings 2020). Users should, therefore, devise strong passwords or passphrases, which may deter phishers' efforts to launch a successful attack (NCSC 2018). Verification of the user can also be accomplished by combining something that only the user knows (e.g., passwords), possesses (e.g., a code), or exhibits as an inherent bodily feature (e.g., fingerprints, retina/iris patterns) (CISA 2020; Stallings 2020). The multifactor authentication of knowledge, possession, and inherence relevant to the user is recommended as an essential tool (CISA 2020) in place of the previously utilized two-factor authentication.

Situational control objective 4: limit phishers' ability to find sensitive information

When phishers attempt to access PII, their ability to locate it or sensitive information belonging to the organization will be reduced if the appropriate procedures are



in place. Access control⁶ and network and database security may be appropriate additional defenses against extraction of PII.

Access control

Granting users access only to needed files and programs while restricting access to sensitive information to those with specially assigned privileges may minimize the risk of penetration by adversaries (CISA 2020). Requiring multiple people to sign off on granting access to sensitive data may also be prudent in safeguarding the organization's assets. Limiting users' access to local networks or virtual private networks (VPNs) may offer further safeguards against phishers.

Network security

Network segregation separates sensitive servers from publicly accessible ones. Sensitive network assets can be separated from the rest of the network by placing firewalls between them and other servers. In extreme cases, they can be completely disconnected from the rest of the network. Servers that must be accessed both by Internet users and sensitive servers can be placed in a special network compartment called a demilitarized zone (DMZ) (Stouffer et al. 2011; Tracy et al. 2002). Servers in the DMZ can connect to users on the Internet through a firewall and to sensitive servers through a separate firewall. Firewalls provide a "controlled link" between the network and the Internet, as well as a "single choke point" where security protocol can be implemented (Stallings 2020, p. 155). When network segregation is in place, phishers must defeat several network security barriers before they can access sensitive servers (National Security Agency 2010).

An intrusion detection system (IDS) and an intrusion prevention system (IPS) may provide additional layers of security by sending system administrators real-time alerts of an unauthorized user's attempts to access the system and by blocking unauthorized and malicious activity (Stallings 2020).

Database security

If a phisher accesses sensitive data, the system administrator can protect it by using encryption. Encryption programs take the original data, called the plaintext, and a secret key as input and output seemingly random blocks of data, called the ciphertext. To recover the plaintext, a decryption program takes the ciphertext and the secret key as input and outputs the plaintext. The secret key is known only to the system administrator or to legitimate users who own the plaintext. To recover the

⁶ Although some elements of access control may correspond to the concept of target hardening in SCP, consistent with cybersecurity and information security practices, we use access control to refer to "the ability to limit and control the access to host systems and applications via communications links" (Stallings 2020, p. 11). See also Hinduja and Kooi (2013) for examples of target hardening and access control in the information security field.



plaintext, a phisher must steal both the ciphertext and the secret key from a legitimate user. Therefore, encryption adds a security layer to sensitive data (Stallings 2006). It is also important for system administrators to backup data and enable automatic updates for all operating systems and software as basic cybersecurity practices (CISA 2021b).

Situational control objective 5: discourage similar attacks

Once the phisher has exited the system, it may be appropriate to share the general characteristics of phishing attacks as a lessons-learned report to reduce similar future attacks. However, system administrators may wish to consider security and liability issues before revealing the specifics of exploited vulnerabilities (Cichonski et al. 2012). For example, revealing the actual content of a malicious attachment might offer potential phishers clues to further exploit the vulnerability before security patches are deployed. Likewise, a nondisclosure agreement may prohibit system administrators from disclosing the details of a phishing attack that has impacted the confidentiality of the organization's sensitive information (Cichonski et al. 2012). Accessing the IT site for the latest security requirements or trends via VPN only may further ensure that the organization's information infrastructure remains protected from those who have no business accessing its IT-related information.

Although the potential to be compromised by phishing emails is always present due to human and environmental vulnerabilities, mitigation measures at various sequential points as described above should be sufficient to assess current cybersecurity practices and guide the selection and implementation of any additional security protocols.

Conclusion

Phishing emails may appear to be merely a nuisance; however, their potential blow to an individual's PII and an organization's information infrastructure and assets can be costly. In this paper, we have presented a series of mitigation points for phishing attacks and corresponding countermeasures as an incident progresses, with the goal of gaining a systematic understanding of phishing emails by revealing both human and environmental vulnerabilities. The application of a sequential schema from the situational crime prevention approach also facilitates a holistic understanding of phishing emails from cybersecurity and criminological perspectives. For cybersecurity professionals, our model may offer an additional tool to assess existing security measures with a particular focus on appropriate mitigation measures as a security incident progresses. Criminologists and other academic researchers may further advance the utility of the situational crime prevention approach in analyzing and preventing other criminal events, especially those commonly connected to phishing emails, such as identity theft and other identity-based fraud. The mounting evidence of increased volumes of phishing emails, subsequent cybersecurity issues, monetary losses for organizations, and criminal organizations' involvement in identity theft



stemming from human and environmental vulnerabilities should drive all concerned stakeholders to engage in the greatly needed theory-driven and empirically based research that will help us address a host of vital issues surrounding phishing attacks.

Acknowledgements The authors would like to thank Bruce Barron and Martha Smith for their helpful comments on earlier drafts of this paper. The authors also express their appreciation to the anonymous reviewers for their valuable suggestions.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

- Akiyama, M., T. Yagi, T. Hariu, and Y. Kadobayashi. 2018. HoneyCirculator: Distributing credential honeytoken for introspection of web-based attack cycle. *International Journal of Information Security* 17 (2): 135–151.
- Anti-Phishing Working Group. 2020. *Phishing activity trends report: 3rd quarter 2020*. https://docs.apwg.org/reports/apwg_trends_report_q3_2020.pdf. Accessed 3 Feb 2021.
- Back, S., and J. LaPrade. 2020. Cyber-situational crime prevention and the breadth of cybercrimes among higher education institutions. *International Journal of Cybersecurity Intelligence and Cybercrime* 3 (2): 25–47.
- Bergholz, A., J. De Beer, S. Glahn, M.F. Moens, G. Paab, and S. Strobel. 2010. New filtering approaches for phishing email. *Journal of Computer Security* 18: 7–35. <https://doi.org/10.3233/JSC-2010-0371>.
- Better Business Bureau. 2019. *Is that email really from “the boss?” The explosion of business email compromise (BEC) scams*. <https://www.bbb.org/article/news-releases>. Accessed 8 Mar 2021.
- Bhadane, A., and S.B. Mane. 2017. State of research on phishing and recent trends of attacks. *i-Manager's Journal on Computer Science* 5 (4): 14–35.
- Bossler, A. 2020. Contributions of criminological theory to the understanding of cybercrime offending and victimization. In *The human factor of cybercrime*, ed. R. Leukfeldt and T.J. Holt, 29–59. Abingdon-on-Thames: Routledge.
- Brubaker, N., Zafra, D. K., Lunden, K., Proska, K. and Hildebrandt, C. 2020 *Financially motivated actors are expanding access into OT: Analysis of kill lists that include OT processes used with seven malware families, 2020*. <https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html>. Accessed 2 Feb 2021.
- Button, M., and C. Cross. 2017. *Cyber frauds, scams and their victims*. Abingdon-on-Thames: Routledge.
- Cichonski, P., Millar, T., Grance, T. and Scarfone, K. 2012. *Computer security incident handling guide: Recommendations of the National Institute of Standards and Technology*. U.S. Department of Commerce. Special publication 800-61, Revision 2.
- Clarke, R.V. 1983. Situational crime prevention: Its theoretical basis and practical scope. *Crime and Justice* 4: 225–256.
- Clarke, R.V. 1992. Introduction. In *Situational crime prevention: Successful case studies*, ed. R.V. Clarke, 3–36. Guilderland: Harrow and Heston.
- Clarke, R.V. 1997. Introduction. In *Situational crime prevention: Successful case studies*, ed. R.V. Clarke, 1–43. Guilderland: Harrow and Heston.
- Clarke, R.V., and R. Homel. 1997. A revised classification of situational crime prevention techniques. In *Crime prevention at a crossroads*, ed. S.P. Lab, 17–27. Greenbelt: Academy of Criminal Justice Sciences and Anderson.
- Cohen, L.E., and M. Felson. 1979. Social change and crime rate trends: A routine activity approach. *American Sociological Review* 44 (August): 588–608.



- Congressional Research Service. 2021. *Colonial Pipeline: The DarkSide strikes*. <https://crsreports.congress.gov>. Accessed 12 July 2021.
- Cornish, D. 1994. The procedural analysis of offending and its relevance for situational prevention. In *Crime prevention studies*, vol. 3, ed. R. Clarke, 151–196. New York: Criminal Justice Press.
- Cornish, D.B., and R.V. Clarke. 1987. Understanding crime displacement: An application of rational choice theory. *Criminology* 25 (4): 933–948.
- Cornish, D.B., and R.V. Clarke. 2003. Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies* 16: 41–96.
- Cybersecurity & Infrastructure Security Agency. 2020. *Cyber essentials toolkit chapter 4: Your surroundings*. https://www.cisa.gov/sites/default/files/publications/cyber%20Essentials%20Toolkit%204%2020200818_508.pdf. Accessed 18 Nov 2020.
- Cybersecurity & Infrastructure Security Agency. 2021a. *Significant historical cyber-intrusion campaigns targeting ICS*. <https://us-cert.cisa.gov/ncas/current-activity/2021/07/20/significant-historical-cyber-intrusion-campaigns-targeting-ics>. Accessed 20 Jul 2021.
- Cybersecurity & Infrastructure Security Agency. 2021b. *Cyber essentials starter kit: The basics for building a culture of cyber readiness*. <https://www.cisa.gov/Cyber-Essentials>. Accessed 8 Mar 2021.
- Cybersecurity & Infrastructure Security Agency. n.d. *CISA Insights: Enhance email & web security*. https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-EnhanceEmailandWebSecurity_S508C-a.pdf. Accessed 17 Nov 2020.
- Eklblom, P. 2017. Crime, situational prevention and technology: The nature of opportunity and how it evolves. In *The Routledge handbook of technology, crime and justice*, ed. M.R. McGuire and T.J. Holt, 353–374. London: Routledge.
- El Aassal, A., S. Baki, A. Das, and R.M. Verma. 2020. An in-depth benchmarking and evaluation of phishing detection research for security needs. *IEEE Access* 8: 22170–22192.
- Federal Bureau of Investigation. 2006. *Financial crimes report to the public*. U.S. Department of Justice. https://fbi.gov/file-repository/stats-services-publications-fcs_report2006-financial-crimes-report-to-the-public-2006-pdf/view Accessed 8 Apr 2020.
- Federal Bureau of Investigation. 2021a. *Internet crime report 2020*. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf Accessed 17 Mar 2021.
- Federal Bureau of Investigation. 2021b. *Increase in PYSA ransomware targeting education institutions*. Alert number CP-000142-MW. <https://www.ic3.gov/Media/News/2021/210316.pdf>. Accessed 7 Apr 2021.
- Federal Bureau of Investigation. n.d. *Scams and safety*. <https://fbi.gov/scams-and-safety/common-scams-and-crimes/identity-theft>. Accessed 11 Feb 2021.
- Federal Bureau of Investigation and Cybersecurity & Infrastructure Security Agency. 2021. *DarkSide ransomware: Best practices for preventing business disruption from ransomware attacks*. https://us-cert.cisa.gov/sites/default/files/publications/AA21-131A_Darkside_Ransomware.pdf. Accessed 12 July 2021.
- Federal Trade Commission. 2021. *Consumer sentinel network: Databook 2020*. <https://www.ftc.gov/data>. Accessed 1 Mar 2021.
- FinCEN. 2020. *Advisory on cybercrime and cyber-enabled crime exploiting the Coronavirus disease 2019 (COVID-19) pandemic*. FIN-2020-A005.
- Finklea, K. 2014. *Identity theft: Trends and issues*. Congressional Research Service.
- FireEye Mandiant Services. 2021. *M-Trends 2021*. <https://www.fireeye.com/current-Threats/annual-threat-report/mtrends.html>. Accessed 14 July 2021.
- FortiNet Guard Labs. 2020. *EKANS ransomware targeting OT ICS systems*. <https://www.fortinet.com/blog/threat-research/ekans-ransomware-targeting-ot-ics-systems>. Accessed 9 Feb 2021.
- Fung, B. and Sands, G. 2021. *Ransomware attackers used compromised password to access Colonial Pipeline network*. <https://www.cnn.com/2021/06/04/politics/colonial-pipeline-ransomware-attack-password/index.html>. Accessed 12 Jul 2021.
- Gajek, S. and Sadeghi, A. R. (2007) A forensic framework for tracing phishers. In *IFIP International Summer School on the Future of Identity in the Information Society* (pp. 23–35). Springer.
- Green, B., S. Gies, A. Bobnis, N.L. Piquero, A.R. Piquero, and E. Velasquez. 2020. Exploring identity-based crime victimizations: Assessing threats and victim services among a sample of professionals. *Deviant Behavior*. <https://doi.org/10.1080/01639625.2020.1720938>.
- Greenman, C., R. Johnson, and D. Esplin. 2021. Cyberattacks in higher education at an epidemic level. *Fraud Magazine* 36 (1): 12–15.



- Gupta, B.B., N.A.G. Arachchilage, and K.E. Psannis. 2018. Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunication Systems* 67: 247–267. <https://doi.org/10.1007/s11235-017-0334-z>.
- Hartel, P., M. Junger, and R. Wieringa. 2011. *Cyber-crime science = crime science + information security*. London: University of Twente.
- Hinduja, S., and B. Kooi. 2013. Curtailing cyber and information security vulnerabilities through situational crime prevention. *Security Journal* 26: 383–402.
- HP-Bromium. 2020. *Threat insights report, Q4–2020*. https://threatresearch.ext.hp.com/wp-content/uploads/2021/03/HP_Bromium_Threat_Insights_Report_Q4_2020.pdf. Accessed 17 Mar 2021.
- Hu, H. and Wang, G. 2018. *End-to-end measurements of email spoofing attacks*. In Proceedings of the 27th USENIX Security Symposium. <https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-hu.pdf>. Accessed 2 Mar 2019.
- Hough, J.M., R.V.G. Clarke, and P. Mayhew. 1980. Introduction. In *Designing out crime*, ed. R.V.G. Clarke and P. Mayhew, 1–17. London: Her Majesty's Stationery Office.
- Jones, B.D. 1999. Bounded rationality. *Annual Review of Political Science* 2: 297–321.
- Karim, A., S. Azam, B. Shanmugam, K. Kannoorpatti, and M. Alazab. 2019. A comprehensive survey for intelligent spam email detection. *IEEE Access* 7: 168261–168295.
- Kratikal. 2020. *Staggering phishing statistics in 2020*. <https://www.kratikal.com/blog/Staggering-phishing-statistics-in-2020/>. Accessed 10 Feb 2021.
- Lazarov, M., Onaolapo, J. and Stringhini, G. 2016. *Honey sheets: What happens to leaked Google spreadsheets?* In Proceeding of the 9th Workshop on Cyber Security Experimentation and Test. <https://www.usenix.org/system/files/conference/cset16/cset16-paper-lazarov.pdf>. Accessed 1 Sep 2019.
- Nanduru, B. 2021. *Take it personally: Ten tips for protecting your personally identifiable information*. National Cybersecurity Alliance. <https://staysafeonline.org/blog/ten-tips-for-protecting-your-pii/>. Accessed 23 Aug 2020.
- National Conference of State Legislatures. 2020. *State laws addressing “phishing.”* <https://www.ncsl.org/research/telecommunications-and-information-technology/state-phishing-laws.aspx>. Accessed 11 Feb 2021.
- National Cyber Security Centre. 2018. *Phishing attacks: Defending your organization*. <https://ncsc.gov.uk/guidance/phishing>. Accessed 15 Oct 2020.
- National Institute of Standards and Technology. 2018. *Framework for improving critical infrastructure cybersecurity*. Version 1.1. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>. Accessed 17 Jul 2021.
- National Security Agency. 2010. *Defense in depth*. <https://apps.nsa.gov/iaarchive/library/ia-guidance/archive/defense-in-depth.cfm>. Accessed 11 Mar 2019.
- Oest, A., Safei, Y., Doupe, A., Ahn, G. J., Wardman, B. and Warner, G. 2018. *Inside a phisher's mind: Understanding the anti-phishing ecosystem through phishing kit analysis*. In Proceedings of the 2018 APWG Symposium on Electronic Crime Research. <https://docs.apwg.org/ecrimeresearch/2018/5349207.pdf>. Accessed 1 June 2020.
- Oest, A., Safaei, Y., Zhang, P., Wardman, B., Tyers, K., Shoshitaishvili, Y. and Doupe, A. 2020a. *Phish-time: Continuous longitudinal measurement of the effectiveness of anti-phishing blacklists*. In Proceedings of the 29th USENIX Security Symposium. <https://www.usenix.org/system/files/sec20-oest-phishtime.pdf>. Accessed 1 Nov 2020.
- Oest, A., Zhang, P., Wardman, B., Nunes, E., Burgis, J., Zand, A., Thomas, K., Doupe, A. and Ahn, G.J. 2020b. *Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale*. In Proceedings of the 29th USENIX Security Symposium. <https://www.usenix.org/conference/usenixsecurity20/presentation/oest-sunrise>. Accessed 10 Oct 2020.
- Parker, D.B. 1998. *Fighting computer crime: A new framework for protecting information*. New York: Wiley.
- Payne, B.K., and L. Hadzhidimova. 2020. Disciplinary and interdisciplinary trends in cybercrime research: An examination. *International Journal of Cyber Criminology* 14 (1): 81–105.
- Peng, P., Xu, C., Quinn, L., Hu, H., Viswanath, B. and Wang, G. (2019) *What happens after you leak your password: Understanding credential sharing on phishing sites*. In: Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security. <https://people.cs.vt.edu/pengp17/papers/asiaccs19.pdf>. Accessed 1 June 2020.
- Proofpoint. 2021a. *2021 State of the phish: An in-depth look at user awareness, vulnerability and resilience*. <https://www.proofpoint.com>. Accessed 11 Feb 2021.



- Proofpoint. 2021b. *Q4 2020 threat report: A quarterly analysis of cybersecurity trends, tactics and themes*. <https://www.proofpoint.com/us/blog/threat-insight/q4-2020-threat-report-quarterly-analysis-cybersecurity-trends-tactics-and-themes>. Accessed 25 Feb 2021.
- Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., Duezguen, R., Lofthouse, B., von Landesberger, T. and Volkamer, M. 2020. *An investigation of phishing awareness and education over time: When and how to best remind users*. In: Proceedings of the 16th USENIX Symposium on Usable Privacy and Security. https://www.usenix.org/system/files/soups2020-reinheimer_0.pdf. Accessed 10 Oct 2020.
- Reyns, B.W. 2010. A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. *Crime Prevention and Community Safety* 12: 99–118.
- Rustad, M.L. 2019. *Global Internet law in a nutshell*, 4th ed. St. Paul: West Academic Publishing.
- Secureworks. 2019. *Resurgent Iron Liberty targeting energy sector*. Counter Threat Unit Research Team. <https://www.secureworks.com/research/resurgent-iron-liberty-targeting-energy-sector>. Accessed 14 July 2021.
- Simon, H.A. 1955. A behavioral model of rational choice. *Quarterly Journal of Economics* 69 (1): 99–118.
- Simon, H.A. 1957. *Models of man*. New York: Wiley.
- Singh, K., Aggarwal, P., Rajivan, P. and Gonzalez, C. 2019. *Training to detect phishing emails: Effects of the frequency of experienced phishing emails*. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (vol. 63, no. 1, pp. 453–457). Sage.
- Smith, M.J., and R.V. Clarke. 2012. Situational crime prevention: Classifying techniques using “good enough” theory. In *Oxford Handbook of crime prevention*, ed. B.C. Welsh and D.P. Farrington, 291–315. Oxford: Oxford University Press.
- Stallings, W. 2006. *Cryptography and network security*, 4th ed. London: Pearson.
- Stallings, W. 2020. *Information privacy engineering and privacy by design: Understanding privacy threats, technology, and regulations based on standards and best practices*. Boston: Addison-Wesley.
- Steves, M., K. Greene, and M. Theofanos. 2020. Categorizing human phishing difficulty: A Phish Scale. *Journal of Cybersecurity*. <https://doi.org/10.1093/cybsec/tyaa009>.
- Stouffer, K., Falco, J. and Scarfone, K. (2011) *Guide to industrial control systems (ICS) security*. NIST Special Publication 800–82. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf>. Accessed 12 Dec 2020.
- Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G. and Thomas, C. B. (2020) *MITRE ATT&CK: Design and philosophy*. MITRE Corporation.
- Thompson, C., Shelton, M., Stark, E., Walker, M., Schechter, E. and Felt, A. P. 2019. *The web's identity crisis: understanding the effectiveness of website identity indicators*. In Proceedings of the 28th USENIX Security Symposium. <https://www.usenix.org/system/files/sec19-thompson.pdf>. Accessed 12 Dec 2020.
- Tracy, M., Jansen, W. and McLarnon, M. 2002. *Guidelines on securing public web servers*. NIST Special Publication 800–44. Version 2.
- Travelers Risk Control. 2016. *Where is your supply chain the most vulnerable?* [Infographic]. Travelers Insurance. <https://www.travelers.com/resources/supply-chain-management/where-is-your-supply-chain-most-vulnerable>. Accessed 7 Apr 2020.
- U.S. Department of Homeland Security. 2021. *DHS announces new cybersecurity requirements for critical pipeline owners and operators*. <https://www.dhs.gov/news/2021/05/27/hds-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators>. Accessed 20 July 2021.
- U.S. Department of Homeland Security. 2021b. *DHS announces new cybersecurity requirements for critical pipeline owners and operators*. <https://www.dhs.gov/news/2021/07/20/hds-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators>. Accessed 20 July 2021.
- U.S. Department of Justice. 2014. *Leader of identity theft ring sentenced for stealing more than 600 identities and causing more than \$1 million in losses*. Office of Public Affairs. <https://www.justice.gov/opa/pr/leader-identity-theft-ring-sentenced-stealing-more-600-identities-and-causing-more-1-million>. Accessed 3 Mar 2020.
- U.S. Department of Justice. 2017. *Russian cyber-criminal sentenced to 14 years in prison for role in organized cybercrime ring responsible for \$50 million in online identity theft and \$9 million bank fraud conspiracy*. Office of Public Affairs. <https://www.justice.gov/opa/pr/russian-cyber-criminal-sentenced-14-years-prison-role-organized-cybercrime-ring-responsible>. Accessed 3 Mar 2020.



- U.S. Department of Justice. 2021. *U.S. government launches first one-stop ransomware resource at StopRansomware.gov*. Office of Public Affairs. <https://www.justice.gov/opa/pr/us-government-launches-first-one-stop-ransomware-resource-stopransomwaregov>. Accessed 15 July 2021.
- U.S. Secret Service. 2020. *Secret Service issues COVID-19 (Coronavirus) phishing alert* [Press release]. <https://www.secretservice.gov/press/releases/2020/03/secret-service-issues-covid-19-coronavirus-phishing-alert>. Accessed 7 Apr 2020.
- Verizon. 2020. Data breach investigations report. <https://enterprise.verizon.com/resources/reports/2020/2020-data-breach-investigations-report.pdf>. Accessed 8 Dec 2020.
- Willison, R., and J. Backhouse. 2006. Opportunities for computer crime: Considering systems risk from a criminological perspective. *European Journal of Information Systems* 15: 403–414.
- Willison, R., and M. Siponen. 2009. Overcoming the insider: Reducing employee computer crime through situational crime prevention. *Communication of the ACM* 52 (9): 133–137.
- Wortley, R. 2001. A classification of techniques for controlling situational precipitators of crime. *Security Journal* 14 (4): 63–82.
- Xiong, A., R.W. Proctor, W. Yang, and N. Li. 2017. Is domain highlighting actually helpful in identifying phishing web pages? *Human Factors* 59 (4): 640–660.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

