Winter 12-13-2018

A Taxonomy of Phishing: Attack Types Spanning Economic, Temporal, Breadth, and Target Boundaries

Daniel Pienta
Clemson University

Jason Bennett Thatcher
The University of Alabama

Allen C. Johnston
The University of Alabama

A Taxonomy of Phishing: Attack Types Spanning Economic, Temporal, Breadth, and Target Boundaries

Daniel Pienta[1]
Clemson College of Business, Clemson University
Clemson, SC, United States

Jason Bennett Thatcher
The Culverhouse College of Business, The University of Alabama,
Tuscaloosa, AL, United States

Allen C. Johnston
The Culverhouse College of Business, The University of Alabama
Tuscaloosa, AL, United States

ABSTRACT

Phishing remains a pernicious problem for organizations. Phishing attacks are increasing in sophistication, which hinders the ability of cybersecurity functions to effectively defend against them. These attacks are becoming increasingly complex, dynamic, and multifaceted to evade the organizational, individual, and technical countermeasures employed in a cybersecurity ecosystem. Information security (ISec) phishing research and practice have provided an understanding of generalized phishing attacks and their subsequent defense. Yet by applying generalized phishing rules to these studies, it may not be sufficient to understand and defend escalated forms of phishing. This study seeks to develop a taxonomy of phishing to provide a more nuanced understanding of this phenomena. This taxonomy may assist ISec research in providing theoretical guidance for the understanding and defense of the various forms of phishing.

[1] Daniel Pienta. dpienta@clemson.edu

Keyword: Phishing, Taxonomy, Cybersecurity, Whaling, Cloning, Social Engineering

INTRODUCTION

Phishing persists as a problem for cybersecurity, as 98% of socially engineered breaches utilize some form of phishing, with email being the most common attack vector (Verizon 2018). In fact, 30% of phishing emails that bypass technical countermeasures are opened by targeted users and 12% of those users click on a malicious attachment or link (Verizon 2018). Typically, phishing messages imitate a trustworthy source and request information via some form of electronic communication (Wright et al. 2014; Jakobsson and Myers 2007). Phishing, when successfully executed, is extremely profitable for cyber criminals, with the average cost to a victimized mid-size company being $1.6 million dollars.

Phishing attacks are increasing in sophistication, utilizing different payloads and targeting a broader range of victims and assets. For example, in an attack targeting a mass population, cyber criminals attacked user Gmail accounts[2]. This attack rifled through inbox, sent, and draft mail folders to propagate an email request to access a shared Google document that afforded access to the victim's Google contacts and Google Drive. In a more targeted attack on the CEO of Facc AG, an Austrian aircraft parts manufacturer, cyber criminals used a highly customized email to trick the CFO into transferring an estimated $50 million US dollars into an undisclosed account[3]. This highly customized phishing attack resulted in the dismissal of both the CEO and CFO because they were negligent in preparing the company for such an attack.

Although mass and specific phishing attacks are very different, defenses often fail because they rely on generalized phishing rules (i.e. relatively simple heuristics for how to identify phishing). Many practitioner phishing training programs rely on the user to 1) ensure the

[2] From 2017: https://www.nytimes.com/2017/05/03/technology/personaltech/email-attack-hits-google-what-to-do-if-you-clicked.html

[3] Obtained from: https://www.scmagazineuk.com/aeroplane-part-maker-claims-cyber-fraud-cost-it-50-million/article/531394/. Also, it should be noted that attack details in these highly specialized attacks typically remain confidential to the organization.

email header is legitimate not impersonated 2) hover and ensure an embedded link is legitimate 3) review the domain name for legitimacy 4) review for generic salutations 5) review for spelling errors, and 6) look for urgent requests for sensitive information. Cognitively, it is difficult to believe users can apply such sophisticated sets of rules while also performing their assigned work. The difficulty of applying generalized phishing rules is compounded by the sheer volume of dynamic phishing attacks, which rely on general rules to identify phishing messages, resulting in technical solution detection success rates hovering at 90% (Hong et al. 2012), thus leaving the organization at risk.

Some academic studies have examined how to design phishing countermeasures such as training, motivation, fear appeals, and threat identification (Abbasi et al. 2015; Schuetz et al. 2016; Wright et al. 2014; Jensen et al. 2017), as well as the tactics utilized by cyber criminals to craft effective phishing messages (Wright et al. 2014; Wright and Marett 2010). Often, to ensure ecological validity, these studies mirror generalized rules employed in the design of phishing training (Dodge et al. 2007; Jagatic 2007; Wright and Marett 2010; Hong 2012; Wright et al. 2014; Wang et al. 2017). Perhaps due to the volume of messages and the dynamic evolution of phishing, information security research (ISec) provides limited guidance to practitioners for how to effectively respond to increasingly complex phishing attacks or how to contextualize countermeasures to prevent different types of phishing attacks.

Developing a more nuanced understanding of phishing and how to select countermeasures, is important because understanding the underpinnings of different phishing attacks will provide theoretical guidance for how to develop defense against them. In this study, we begin to develop a comprehensive phishing taxonomy based on academic ISec research and knowledge from practice in order to offer a research agenda for future phishing studies (Table 1).

In doing so, we suggest that the ISec community go beyond PMT to examine novel theoretical mechanisms to elicit compliance with security policies. By doing so, we take a first step towards developing a theoretical understanding of the intricacies of the many forms of phishing and provide a means to evaluate the applicability of different countermeasures.

Table 1. Key Phishing Literature

Source	Journal	Theory	Phishing Attack	Countermeasure		Behavior
				Deployed	Stimulated	
Wang et al. (2017b)	JAIS	Overconfidence	Phishing	N/A	Judgement	Detection
Wang et al. (2017a)	ISR	Coping & Extended Parallel Process Model (PMT Extension)	Spear Phishing	Coping Adaptiveness	Awareness	Detection Effort & Accuracy
Jensen et al. (2017)	JMIS	Mindfulness	Phishing & Spear Phishing	Mindfulness/ Awareness	Training	Avoidance of phishing email
Schuetz et al. (2016)	PACIS Proceedings	Construal Level & Protection Motivation	Spear Phishing	Fear Appeal (Policy)	Training	Download further phishing training
Zahedi et al. (2015)	JAIS	Protection Motivation	Fake Website (Pharming)	Anti-Phishing Detector	Awareness	Avoidance of phishing website
Abbasi et al. (2015)	JMIS	Genre Theoretic Perspective	Fake Website	Anti-Phishing Detector	Awareness	Avoidance of pharming website
Wright et al. (2014)	ISR	Persuasion & Motivation	Spear Phishing	N/A	N/A	Avoidance of phishing email
Arachchilage & Love (2014)	Computer in Human Behavior	Technology Threat Avoidance	Phishing	Avoidance Motivation	Training & Motivation	Avoidance of phishing email
Abbasi et al. (2012)	ISI 2012	N/A	Fake Website (Pharming)	Anti-Phishing Detector	Awareness	Avoidance of pharming website
Wright & Marett (2010)	JMIS	Interpersonal Deception Theory	Spear Phishing	N/A	N/A	Avoidance of phishing email
Kumaraguru et al. (2010)	ACM Trans. Intern. Tech	Instructional Design	Phishing	Training	Training	Avoidance of phishing email
Dodge et al. (2007)	Computers and Security	N/A	Spear Phishing (customized)	Training	Training	Avoidance of phishing email
Jagatic et al. (2007)	CACM	N/A	Targeted Phishing	N/A	N/A	N/A

Phishing

Phishing is a form of social engineering utilized by cyber criminals to obtain confidential information from an end user through the imitation of a trustworthy source (Hong 2012; Wright et al. 2014). Phishing attacks typically rely on electronic communications (e.g., email, sms, VOIP, instant messaging, etc.) that appear to be from trusted sources (e.g., financial institution, personal contact, etc.) to deceive the user into clicking on a malicious link or downloading a malicious file (Hong 2012). The majority of phishing attacks unfold in three phases: (1) circumventing technical cybersecurity countermeasures to deliver the deceptive electronic communication to the target, (2) convincing the target into taking the suggested action, and (3) the cybercriminal capitalizing on the delivered payload for payoff. These payoffs can take a number of forms, such as monetary damages, espionage, lost trade secrets, and sabotage, as cyber criminals involved in phishing have various nefarious goals.

Phishing remains popular among cyber criminals for many reasons. First, phishers have access to low-cost tools. The Anti-Phishing Work Group reported 180,577 cyber criminals initiated attacks in quarter four of 2017, targeting over 348 brands, and sending out 233,613 known, unique phishing attempts[4]. Such attacks are enabled by free phishing kits available to cyber criminals available on the light and dark web, enabling out-of-the-box opportunities to conduct malicious phishing campaigns (Cova et al. 2008). Second, as the payoffs from selling credentials and credit cards have decreased on the dark web due excess availability, cyber criminals have directed more attention to focused and complex phishing attacks with potential higher payoffs (Choo 2011). Finally, perhaps due to weak or unenforced organizational policies, users remain a weak link in security as an estimated 90% of data breaches result from socially engineered cyber-attacks (Wright et al. 2014).

[4] Obtained from the APWG phishing trends report 4th quarter 2017. http://docs.apwg.org/reports/apwg_trends_report_q4_2017.pdf

To mitigate phishing attacks, security professionals and academics have developed generalizable, multi-tiered approaches to implementing countermeasures. These countermeasures operate on three levels: technical (e.g., firewalls, encryption software, blacklisting, blocking, two factor authentication), individual (e.g., SETA programs, training, motivation), and organizational (e.g., prosecution, investments, legal, policy). For instance, if a phishing email penetrates a technical countermeasure, an individual may rely on past training to identify the email. If the phishing attack is successful, an organization, upon identifying the culprit of the attack, may seek justice and restitution through legal means in order to deter future attacks. In developing these holistic defenses to phishing, many organizations rely on recommendations to use turnkey sets of tools and practices to tie together technology, people, processes, and information and defend their perimeters[5].

To circumvent increasingly sophisticated countermeasures, cyber criminals have designed highly complex phishing attacks that take advantage of known features of even the most touted defenses. Consider two factor authentication (2FA), a technical countermeasure. 2FA provides an extra layer of security beyond a username and password, by requiring information pushed to a user on a device (e.g. sending a code via a cell phone). 2FA was recently weaponized by cyber criminals via social engineering tactics[6]. Cyber criminals obtain the 2FA session cookie by redirecting the end user to a spoofed login page where they pass credentials (login, password, and 2FA authentication code) through to the authentic website, thereby securing a session cookie and login. Note, this does not imply the technical countermeasure failed, rather the security breach occurs because an individual clicks on a malicious link or downloads malware via phishing. Realizing a richer understanding of how cyber criminals

[5] Based on the 2017 phishing defense guide: https://www.ciosummits.com/PhishMe-Phishing-Defense-Guide_2017.pdf

[6] Obtained from https://techcrunch.com/2018/05/10/hacker-kevin-mitnick-shows-how-to-bypass-2fa/

bypass countermeasures' features to reach users, through a more nuanced understanding of the different types of phishing, will afford opportunities to further refine countermeasures necessary to secure firm boundaries.

In summary, phishing continues to be a pervasive danger to organizations, resulting in a myriad of economic losses and continuing to evolve in complexity. Efforts have been made by academics, practitioners, and governments to defend against phishing attacks through individual, technical, and organizational countermeasures, yet phishing continues to remain a potent tool for cyber criminals. This may be due to the continued evolution of phishing, to take advantage of known features of countermeasures, to target specific individuals or to integrate new methods. Therefore, ISec research needs to develop an updated, thorough understanding of phishing attacks in order to extend current theoretical understanding of this phenomenon to develop more effective defense of this phenomena.

Phishing in ISec Literature

ISec researchers have directed much attention to phishing, employing diverse methods ranging from economic modeling to psychometric analysis and field experiments. ISec researchers have typically sought to test, develop, and/or analyze a set of technical and individual countermeasures that validate their methods by detecting general phishing messages or evaluating their impact on known sets of security policies/steps. By doing so, ISec research seeks to provide advice on how to develop effective countermeasures to defend against phishing attacks.

ISec research has extensively investigated technical phishing countermeasures. Abbasi et al. (2010) used statistical learning theory (SLT) to develop a new class of fake website detection systems. Through a series of experiments, this research showed that systems grounded in SLT

have more efficacy in detecting websites since they use a richer set of fraud cues and domain specific knowledge. Furthering this work, Abbasi et al. (2015) used a genre tree kernel method to improve detection of phishing websites by end users compared to state-of-the-art anti-phishing methods in practice. Additionally, Vance et al. (2014) studied users habituation and disregard to information systems warnings, such as the technological interjections phishing system rely upon. The findings suggest that over time individuals become desensitized to these warnings and therefore there is a need for improvements in the design of these warnings (Anderson et al. 2016; Vance et al. 2014).

ISec research has also investigated phishing countermeasures from an individual perspective, looking at how training, influence tactics, and motivation, among others, affect users ability and intention to identify, detect, and protect confidential information (Schuetz et al. 2016; Wright et al. 2014; Wright and Marett 2010). For instance, Wright et al. (2014), through a field experiment, studied the effects of influence tactics employed by cyber criminals in phishing. This research extended theoretical understanding of persuasion and motivation theories, in the context of phishing, by identifying which persuasive tactics were most efficacious in a successfully phishing attack. At the same time, this research provided guidelines for cybersecurity departments to defend these attacks by noting the use of these tactics in phishing emails. The practical impact of this work can be seen in online corporate training providers, like LawRoom, where they are now incorporating influence techniques into training modules.

ISec phishing research has directed attention to phishing countermeasures from an organizational perspective. Dey et al. (2014) looked at various forms of cybersecurity software, including anti-phishing, and found that network effects work as a counterweight, which provides vendors incentive to collocate at the top end of the quality spectrum. This provides vendors a

reason to not differentiate their product and move anti-phishing software forward, since they do not receive a monetary incentive. This shows that organizations need to be strategic in their choice of anti-phishing software, as differentiation may not be a driving factor since most software is geared toward mass attacks rather than targeted attacks. Benaroch and Chernobai (2017) found the importance board level governance plays in the number of operational IT failures. This research demonstrated that organizational countermeasures, such a governance, influence defense against IT operational failures, such as the loss of confidential information due to phishing (Benaroch & Chernobai, 2017).

ISec research has also studied general defense strategies relevant to phishing. For instance, behavioral researchers have studied protection motivation theory and its effect on individual motivation behavioral to protect information assets (Boss et al. 2015; Johnston et al. 2015; Johnston and Warkentin, 2010). ISec researchers have also studied the effects of government mandates (Png et al. 2008), enforcement (Willison and Warkentin 2013) and vulnerability disclosure and attack diffusion (Mitra and Ransbotham 2015), among others. Although, these streams are not specifically contextualized to phishing they provide insight into the problem and its defense.

Phishing in Practice

Despite academic research, phishing remains a persistent noxious problem in practice. Many cybersecurity companies offer anti-phishing tools. For example, most email systems build in phishing countermeasures, such as blocking and filtering mechanisms, that remove access to malicious emails and websites. Despite such measures, practitioners note that the majority of employees remain ill prepared to identify an attack and lack general knowledge of cybersecurity (Olmstead and Smith 2017).

In contrast to ISec research, which primarily studies phishing, in general (Abbasi et al. 2015, 2010; Dey et al. 2014; Wright and Marett, 2010), or spear phishing, in particular (Jensen et al. 2017; Schuetz et al. 2016; Wright et al. 2014), practitioner literature focuses on delineating features of, and methods to defend against, novel forms of phishing attacks, as each attack entails different levels of complexity and targets (Rashid 2017, Brecht 2018). They do so, because in order to inoculate users against their effects, practitioners feel they must be able to describe their key features and their potential impact on the organization

Practitioners primarily note the following forms: (1) pharming (2) phishing (3) spear phishing (4) clone phishing, and (5) whaling (Table 2). Pharming refers to the practice of directing internet users to a bogus website that mimics a legitimate one to harvest confidential information. Phishing refers to attempts to acquire confidential information from a mass group of people by masquerading as a trustworthy source. Spear phishing refers to attempts directed at specific individuals within a group using personal information as a means to increase success. Clone phishing refers to replicating a legitimate email and replacing the link or file with a malicious version. Whaling attacks are directed specifically at senior executives or other high profile targets within a business by using highly customized threat intelligence[7]. These forms represent broad categories, and there is a need to develop crisper descriptions and gather details of specific attacks, in order to understand the rate at which they occur and their impact on organizations.

Although the practitioner literature classifies general forms of phishing attacks, it lacks precision necessary to clearly provide a universal understanding of attack characteristics. For example, to a layman, spear phishing may be indistinguishable from clone phishing, leading to

[7] Obtained from general descriptions from phishing defense software providers and practitioner literature: https://www.phishingbox.com/news/phishing-news/types-of-phishing-defined, https://www.csoonline.com/article/3234716/phishing/types-of-phishing-attacks-and-how-to-identify-them.html , https://www.antiphishing.org

confusion among end users about what cues to look for to defend against or a lack of understanding of the implications of responding to one of these ubiquitous persistent threats (Schuetz et al. 2016). A more precise understanding of the different characteristics leading to a classification of the various forms of phishing attacks may provide insight into improving current technical, individual, and organizational phishing defenses.

PHISHING TAXONOMY

In this section, we offer a taxonomy to classify phishing attacks based on ISec research and the practitioner literature. Because ISec research has primarily focused on general phishing and spear phishing, we relied more on the practitioner literature to describe pharming, clone phishing and whaling.

Table 2. A Taxonomy of Phishing

Attack Characteristics	Pharming	Phishing	Spear Phishing	Clone Phishing	Whaling
Target	Random Mass Population (e.g. All visitors of a common website)	Random Mass Population (e.g. All users of Gmail)	Specific Group (e.g. The accounting department of a bank)	Specific Gateway Individual in a Group (e.g. CFO or CEO)	Specific High Value Individual (e.g. C – Level Executives, C-Level Assistants)
Perimeter Spillover	Individualized	Individualized	Organizational Network	Organizational Network	Organizational & Personal Inner and Outer Bands of Network
Instance	Singular	Singular	Singular	Multi-Faceted	Singular or Multi-Faceted
Investment	Minimal (e.g. Craft a spoofed website that mimics a legitimate website and register the domain)	Minimal (e.g. Craft an email about Apple iTunes)	Marginal (e.g. Craft an email to appear from a trustworthy source based on available public data, one time threat intelligence gathering)	Substantial (e.g. multiple machines must be infected, monitoring of the accounts must be conducted, replication must be quick and timely)	Significant (e.g., threat intelligence gathered over time, engagement of multiple communications with target, C&C server for espionage, organizational and personal

					social media account monitoring)
Payoff	Small Incremental Instantiations	Small Incremental Instantiations	Small to Substantial Incremental Instantiations	Substantial One Time or Multiple Instantiations	Significant One Time Monetary Lump Sum
Vulnerable Assets		Information (e.g. credentials, SSN) & Financial	Information (e.g. access to specific database) & Financial	Information (e.g. access to specific database) & Financial	Financial, Reputation (e.g. enticing deviant behavior) , & Human (e.g. ransom a family member)
Artifact	Personalized with general detail	Universal	Personalized with general detail	Identical replication of a legitimate communicatio n	Personalized with finite detail
Payload	Malicious Website (e.g. credential harvesting)	Malicious Link or Malware (e.g. Ransomware)	Malicious Link or Malware (e.g. Ransomware)	Malicious Link or Malware (e.g. Ransomware)	Wire Transfer Request to Criminal Account, Blackmail Information, Location of a Family Member

DISCUSSION

While ISec has a rich tradition of examining phishing attacks, their sources, and their remedies, our study suggests that ISec research has left relatively unexamined important forms of phishing. The majority of ISec research directs attention to individual countermeasures, such as training or motivation, designed to mitigate generalized phishing attacks such as pharming, phishing, or spear-phishing. While our review is preliminary, we believe it suggests several opportunities for future phishing research to address emergent forms of phishing such as cloning and whaling. (Table 3).

First, consistent with recent calls for contextualized theory in the broader IS discipline (Hong et al. 2014), we believe there is a pressing need for developing context-specific theories that provide a more nuanced understanding of different forms of phishing. Such theory development is important, as it may reveal missing relationships and actionable advice for

designing phishing countermeasures. A nuanced understanding of phishing may shed light on when generalized countermeasures are effective (e.g., basic phishing messages), or when firms need to exert more effort to combat specific forms of phishing (e.g., whaling). Further contextualizing existing theories such as PMT may help move ISec research and practice forward in helping to understand how to defend and diffuse different forms of phishing attacks through more contextualized theoretical understanding.

Second, the majority of current research in phishing focuses on an individual, technical, or organization countermeasures in isolation. For example, most approaches that utilize PMT elicit the individual countermeasure of motivation, but absent ability, motivation may not help defend against sophisticated phishing attacks. We believe there is a pressing need for understanding the impact of the intertwinement between different forms of countermeasures, in terms of awareness and access, in shaping user motivation and actual compliance with security policies, particularly for less common, targeted attacks such as whaling.

Third, the majority of phishing field experiments take place during a relatively short amount of time, such as one month, a single-shot exercise, or within a lab environment. In reality, the cybersecurity function of an organization might not have such serendipitous timing, when implementing training, because waiting to send fear inducing warnings, or calls for user action, may result in security breaches. Extended longitudinal research is needed to assess the impact of consistent, sustained security policies vis a vis reactive, emergency interventions. This is particularly important, if we are to understand how to combat recurring (e.g., pharming and spear phishing) as well as episodic threats (e.g., whaling or cloning).

Fourth, there is limited understanding of organizational countermeasures in relation to phishing such as governance, auditing, and policy. Studying the role organizational

countermeasures may play in the different types of phishing attacks could provide insight into how these countermeasures cross organization boundaries. For instance, many organizations have layers of safeguard policies in place to prevent whaling attacks. In many of these attacks, that seek substantial payouts, there is a chain of command protocol in regards to transferring large financial sums. Yet despite such risks, cyber criminals continue to elicit responses from well-placed employees who ignore these human-based protocols and countermeasures.

Lastly, combining theoretical perspectives may shed light on how to effectively design countermeasures (individual, organizational, and technical) and responses to the myriad forms of phishing. For example, in a whaling attack would a more finite understanding of the process used to gather highly customized content provide insight into defenses and subsequent responses to eradicate this phase of the attack? Cloning also relies on highly astute monitoring of networks by cyber criminals typically through the monitoring of multiple email accounts until an action triggers the opportunity to attack. Many of these attacks are carried out through legitimate emails that have been compromised and links are masked within PDF's and other forms that technical countermeasures cannot scan. So extending and combining theory to pre-breach, during breach, and post-breach phases of attack cycles could provide more nuanced understanding of these diverse forms of phishing.

Table 3. Future Phishing Research Directions

Direction	Action	Benefit
Context Specific Theory	Inclusion of multiple forms of phishing	Understanding of the robustness of the proposed theoretical defense
Countermeasure Intertwinement	Inclusion of multiple countermeasures	Understanding of the interaction of different countermeasures
Countermeasure Saliency	Extended longitudinal studies	Understanding of the sustained effects of countermeasures
Organizational Countermeasures	Increased organizational level studies	Understanding of the organizational defense crossing boundaries of the organization

References

Abbasi, A., Zahedi, F., & Chen, Y. (2012, June). Impact of anti-phishing tool performance on attack success rates. In Intelligence and Security Informatics (ISI), 2012 IEEE International Conference on (pp. 12-17). IEEE.

Abbasi, A., Zahedi, F. M., Zeng, D., Chen, Y., Chen, H., & Nunamaker Jr, J. F. (2015). Enhancing predictive analytics for anti-phishing by exploiting website genre information. Journal of Management Information Systems, 31(4), 109-157.

Anderson, B. B., Vance, A., Kirwan, C. B., Jenkins, J. L., & Eargle, D. (2016). From warning to wallpaper: Why the brain habituates to security warnings and what can be done about it. Journal of Management Information Systems, 33(3), 713-743.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior, 38, 304-312.

Benaroch, M., & Chernobai, A. (2017). Operational IT failures, IT value-destruction, and board-level IT governance changes.

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors.

Brecht, D. (2018). Phishing Types. Retrieved from https://resources.infosecinstitute.com/category/enterprise/phishing/spear-phishing-and-whaling/

Dey, D., Lahiri, A., & Zhang, G. (2014). Quality Competition and Market Segmentation in the Security Software Market. Mis Quarterly, 38(2).

Dodge Jr, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. Computers & Security, 26(1), 73-80.

Cova, M., Kruegel, C., & Vigna, G. (2008). There Is No Free Phish: An Analysis of" Free" and Live Phishing Kits. WOOT, 8, 1-8.

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719-731.

Hong, J. (2012). The state of phishing attacks. Communications of the ACM, 55(1), 74-81.

Hong, W., Chan, F. K., Thong, J. Y., Chasalow, L. C., & Dhillon, G. (2013). A framework and guidelines for context-specific theorizing in information systems research. Information Systems Research, 25(1), 111-136.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. Communications of the ACM, 50(10), 94-100.

Jakobsson, M., & Myers, S. (Eds.). (2006). Phishing and countermeasures: understanding the increasing problem of electronic identity theft. John Wiley & Sons.

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. Journal of Management Information Systems, 34(2), 597-626.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. MIS quarterly, 549-566.

Johnston, A.C., Warkentin, M., Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. MIS quarterly, 39(1), 113-134.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. ACM Transactions on Internet Technology (TOIT), 10(2), 7.

Mitra, S., & Ransbotham, S. (2015). Information disclosure and the diffusion of information security attacks. Information Systems Research, 26(3), 565-584.

Olmstead, K., & Smith, A. (2017). Americans and cybersecurity. Pew Research Center, 26.

Png, I. P., Wang, C. Y., & Wang, Q. H. (2008). The deterrent and displacement effects of information security enforcement: International evidence. Journal of Management Information Systems, 25(2), 125-144.

Rashid, F. Y. (2017, October 27). Types of phishing attacks and how to identify them. Retrieved from https://www.csoonline.com/article/3234716/phishing/types-of-phishing-attacks-and-how-to-identify-them.html

Schuetz, S., Lowry, P., & Thatcher, J. (2016). Defending against spear-phishing: Motivating users through fear appeal manipulations.

Vance, A., Anderson, B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). Association for Information Systems.

Wang, J., Li, Y., & Rao, H. R. (2017). Coping responses in phishing detection: an investigation of antecedents and consequences. Information Systems Research, 28(2), 378-396.

Wang, J., Li, Y., & Rao, H. R. (2016). Overconfidence in phishing email detection. Journal of the Association for Information Systems, 17(11), 759.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. MIS quarterly, 37(1).

Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. Journal of Management Information Systems, 27(1), 273-303.

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research note—influence techniques in phishing attacks: an examination of vulnerability and resistance. Information systems research, 25(2), 385-400.

Zahedi, F. M., Abbasi, A., & Chen, Y. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. Journal of the Association for Information Systems, 16(6), 448.