Using stage theorizing to make anti-phishing recommendations more effective

Abstract

Purpose

This paper reviews the behavioral phishing literature to understand why anti-phishing recommendations are not very effective and to propose ways of making the recommendations more effective. The paper also examines how the concept of stages from health communication and psychology can be used to make recommendations against phishing more effective.

Design/Methodology/Approach

This literature review study focused on the behavioral phishing literature that has relied on human subjects. Studies were excluded for reasons that included lacking practical recommendations and human subjects.

Findings

The study finds that phishing research does not consider where victims are residing in qualitatively different stages. Consequently, the recommendations do not often match the specific needs of different victims. This study proposes a prototype for developing stage theories of phishing victims and identifies three stages of phishing victims from analysing the previous phishing research.

Practical implications

The study recommends categorizing individuals into stages, based on their security knowledge and online behaviors, and other similar characteristics they may possess. A stage approach will consider that individuals who at one time clicked on a phishing link because they lacked the

requisite security knowledge, after receiving security training, may click on a link because they are overconfident.

Originality/value

The paper explains why proposing anti-phishing recommendations, based on a "one-size fits all" approach has not been very effective (e.g., because it simplifies why people engage in different behaviors). The proposals introduce a new approach to designing and deploying anti-phishing recommendations based on the concept of stages.

Keywords: phishing, stage theorizing, anti-phishing recommendations, targeted communication/messaging

1. Introduction

Phishing represents a major form of online identity theft that relies on social engineering to deceive people into divulging personal and sensitive information. Victims perceive the phishing messages to be authentic and associated with legitimate persons and organizations. By targeting people, phishers (the perpetrators of phishing emails) circumvent technical measures such as email filters, firewalls, encryption software, and authentication mechanisms that are designed to detect and discard phishing emails before they reach a recipient. The Anti-Phishing Working Group (APWG, 2017) reported a 65% increase in the total number of phishing attacks in their fourth quarterly report (October-December, 2016). Recent industry reports suggest that phishing costs an average 10,000-employee company about USD 3.7 million a year, and that the average employee wastes over four hours a year dealing with phishing attacks (Korolov, 2015).

Over a ten-year period, phishing attacks have significantly increased in sophistication (Hong, 2012). Phishers have evolved their tactics from sending mass-email messages to contextualized messages that use relevant information to deceive the recipients (Goel, Williams, & Dincelli, 2017). Researchers have adopted numerous theoretical perspectives from the fields of psychology and communications research to explain why people become phishing victims and to suggest recommendations to reduce phishing. Evidence, however, suggests that extant anti-phishing recommendations are not very effective (Goel et al., 2017; Tambe Ebot, 2017). Alsharnouby (2015) reported that a decade of improvements in security education and URLs have yielded only a six percent increase in phishing attempt detection rates by users.

The increase in phishing attacks, its sophistication, and the large number of individuals and organizations susceptible to phishing attacks are compelling reasons for developing more effective anti-phishing recommendations. A common misconception in phishing research is that making generic anti-phishing recommendations based on empirical studies is enough to change behaviors and make people identify and avoid phishing attacks.

In the health psychology and communication literature, researchers have found that fully informing individuals about health and health risk does not necessarily lead to a change in behavior in isolation (Whitehead & Russell, 2004; Noar, 2006). Numerous research studies done on health psychology suggests that targeted messages can be more effective than generic messages (Noar, 2006).

This study examines why anti-phishing recommendations have not been very effective and propose measures that can make the recommendations more effective. It is suggested that phishing researchers incorporate the concept of stages from health psychology, and that when making anti-phishing recommendations, researchers should consider that phishing victims may

be residing in different stages (Tambe Ebot, 2017). We examine the following four questions: (1) Why do people fall for phishing attacks? (2) What are the existing recommendations against phishing? (3) Why are the existing recommendations not very effective? (4) How can anti-phishing recommendations be made more effective?

2. A stage approach to phishing recommendations

The phishing literature includes approaches based on many behavioral theories from the fields of communication and psychological research. A common thread that runs through all the research that concerns recommendations that can be deployed to reduce people's susceptibility to phishing attacks is: how can anti-phishing messages that are relevant, informative, and ultimately have the greatest chance of reducing people's susceptibility to phishing attacks be created and deployed? One area of research that has studied such questions is that of health psychology and health communication (Noar, Benac, & Harris, 2007). In health psychology and communication research, researchers prefer using stage-based theories for studying and designing interventions for behavior change and to examine the reasons for the change. For example, stages are typically used to investigate health protective behaviors, such as the adoption of preventive behaviors (Weinstein & Sandman, 1992) and the stopping of unhealthy behaviors (DiClemente et al., 1991; Prochaska, 1994). Stage theories "*assume that behavior change involves movement through a sequence of discrete stages, that different variables influence different stage transitions, and that effective interventions need to be matched to stage*" (Sutton, 2005, p.1).

However, many of the more familiar theories of health behavior (e.g., theory of reasoned action, theory of planned behavior, and protection motivation theory) are labeled as *continuum theories* (Weinstein, Rothman, & Sutton, 1998) or stage-less theories (Velicer & Prochaska, 2008). Continuum models suggest that the way in which the independent variables combine to influence

action is the same for everyone (Schwarzer, 2008). A key difference between stage theories (Schwarzer, 2008) and stage-less theories (Velicer & Prochaska, 2008) is the reasons behind the behavior in question. Continuum models assume that the independent variables are fixed or static, and are applicable indiscriminately to everyone.

Previous phishing research has mainly used continuum models to understand people's reasons for committing security violations and/or not committing security violations. The overwhelming finding from the previous research is that security education is necessary to reduce phishing. In several previous phishing research, where the researchers focused on users with similar characteristics, such as naïve computer users, they reported that participants offered different reasons for clicking on phishing links (Downs, Holbrook, & Cranor, 2006; Egelman, Cranor, & Hong, 2008). Downs et al., (2006) focused on naïve computer users and found that many focused on the email credibility to conclude that the email is relevant to them while others focused on the emails' professionalism to conclude that emails from organizations do not typically have misspellings. Despite the merit of targeting a demographic for phishing research, the researchers did not specify their recommendations based on their participants' reasons for clicking on the phishing links. Downs et al., (2006) emphasized the need for education to begin at the basic level, however, this recommendation does not consider their naïve study participants who possessed more years of Internet experience and were experienced with handling security threats. Furthermore, the extant security education recommendations overlook the fact that the reasons why individuals comply with the phishers' requests may change over time. In addition, phishing victims may be located in different stages, requiring that more effective interventions be matched to their needs based on their respective stage.

Stage theorizing emphasizes the necessity of tailored messages as opposed to more generic messages that are neither targeted, individualized, nor based on any kind of individual assessment (Noar et al., 2007). Generic communication can be personalized by using a characteristic such as a person's name (ibid). However, targeted communication refers to messages developed for a group of individuals or a segment of the population, and they are widely applied in the health education and communication literature (e.g., Kreuter & Wray, 2003; Rimal & Adkins, 2003). Targeted communication is more suitable when it relates to anti-phishing recommendations. It is different from tailored communication and is defined as:

"any combination of strategies and information intended to reach one specific person, based on characteristics that are unique to that person, related to the outcome of interest, and derived from an individual assessment" (Kreuter & Skinner, 2000p. 277).

3. Research Approach

This research followed the procedures for systematic literature review methodology typically used in the health and engineering sciences (Kitchenham, 2004; Okoli, 2015). Okoli (2015) discussed how this methodology can be applied by IS researchers. The focus of the review was to find answers to the following four research questions: (1) why do people fall for phishing attacks? (2) What are the existing recommendations against phishing? (3) Why are the existing recommendations not very effective? (4) RQ 4: How can anti-phishing recommendations be more effective?

I conducted searches for the relevant studies on Google Scholar, and ScienceDirect, and the AIS e-library. Currently, only four phishing studies have been published in some of the major IS

journals. One in *Information Systems Research (Wright, Jensen, Thatcher, Dinger, & Marett, 2014)*, one in *the Journal of Management Information Systems (Wright & Marett, 2010)*, and two in the *Journal of the Association of Information Systems* (Goel et al., 2017; Wang, Li, & Rao, 2016).

The search involved browsing through papers to ascertain that they involved users and were not addressing phishing solely from the perspective of computer science. Each search produced thousands of studies based on many keywords including: "phishing"," behavioral phishing", "phishing and psychology", "users and phishing", "phishing education and training programs", "anti-phishing recommendations", and "why people fall for phishing." For instance, a simple "phishing" search on google scholar yielded 63000 results (5th December, 2017) while a search for "phishing and psychology" yielded over 7000 results (4th December, 2017). The high results for phishing should not be very surprising. The phishing problem is being studied by scholars in many disciplines, such as IS, computer science, engineering, and psychology. The focus of these searches was on empirical behavioral phishing studies that included human subjects as study participants. Therefore, phishing studies that did not rely on human subjects were excluded from this review, such as studies involving the design of filters that automatically detect phishing attacks before they reach the user, or those involving machine learning. Additionally, studies that discussed implementing more effective anti-phishing systems were excluded if the methodology did not include human subjects.

To determine relevant studies, the abstracts were read to determine whether the study involved human subjects and was relevant to the current study. In many instances, after browsing through the abstract, the relevance of a study was also determined by going through the study's methodology and recommendations for practice. The studies listed in Table 1 were read in their

entirety. Furthermore, several studies published in conferences were excluded in favor of the journal versions of the same studies. Similarly, some studies were excluded because of their lack of recommendations for practice (Zhang, Luo, Burd, & Seazzu, 2012). Table 1 contains a description of the findings from empirical phishing studies and their recommendations to reduce phishing.

Table 1. Previous behavioral empirical research phishing

Authors and year	Description/finding of study and recommendation
Alsharnouby, Alaca, & Chiasson, (2015)	**Description and finding:** authors examined whether improved browser security indicators and increased awareness of phishing improve users' ability to protect themselves against phishing. They found that users only successfully detect 53% of phishing websites and they do not spend time looking at security indicators, relying instead on a website's content. **Recommendation:** Humans are unreliable with regards to security. Organizations should automate as much as possible.
Arachchilage, Tarhini, & Love, 2015; Arachchilage & Cole (2016)	**Description and finding:** Authors designed and developed a mobile game prototype as an educational tool. They found that the game prototype improved participants phishing avoidance behavior and their threat perception, safeguard effectiveness, and self-efficacy. **Recommendation:** phishing education and game prototypes should be used to combat phishing.
Alnajim & Munro (2009)	**Description and finding:** authors evaluated the anti-Phishing knowledge retention of users by testing a novel approach against one that relies on sending people anti-phishing messages by email. Authors selected participants who were "phishing unaware" (because they could not define "phishing") despite their technical level. They found that training users many times improved their ability to detect phishing. Users retained their anti-phishing knowledge for 16days. **Recommendation:** authors recommend that anti-phishing training should be an ongoing process.
Pattinson et al. (2012)	**Description and finding:** authors investigated user's responses when either a phishing email or a genuine email arrives in their inbox. They found that users who are familiar with computers and informed about email and social media, manage phishing email better than those who are not informed. **Recommendation:** computer users should be continually reminded that phishing is a serious threat to organizational information security. This should be done through security awareness sessions and risk communication practices.
Dhamija, Tygar, & Hearst (2006)	**Description and finding:** Authors examined why phishing works. They found that good phishing websites are very effective at deceiving their study participants and vulnerability affected everyone irrespective of education, sex, age, previous experience, or hours spent on a computer. **Recommendation:** Phishing should not be approached solely from a traditional cryptography-based security framework. Recommendations should also consider what humans do well and what they do not do well.
Dodge, Carver, & Ferguson (2007)	**Description and finding:** Authors examined the effectiveness of phishing security awareness training through a mocked phishing experiment. Many subjects complied with the phisher's request and submitted personal information. **Recommendation:** Regular phishing email exercises and assessment of long-term retention of anti-phishing training
Downs et al., (2006)	**Description and finding:** authors argue that to develop effective tools that combat phishing, researchers should first understand how and why people fall for phishing attacks.

	They selected naïve participants with little security background knowledge. They found that people may be vulnerable to phishing because they do not link their awareness of phishing to personal vulnerability. While people can manage security risks they are familiar with, they cannot manage phishing attacks that they have not previously encountered. **Recommendation:** authors recommend that developers of tools consider that most users may have little understanding about information related to domain registration, certificates, and other technical concepts. Developers should explain to users what the security tools are used for and how the information is relevant to them. They emphasize that simply teaching people to avoid phishing is unlikely to improve their behavior and recommend that education should start at the basic level.
Egelman et al., (2008)	**Description and finding**: authors examined the effectiveness of web browsers designed with active phishing warnings to determine if, how, and why they fail users. They simulated a phishing attack to expose users to browser warnings. **Recommendation**: web browsers should be designed users' primary task otherwise, they are ineffective. The recommendations should also present the users with clear choices on how to proceed, ensure that users can only proceed to a phishing site after reading the safety message, and security browsers should only be used when there is a clear danger.
Jagatic, Johnson, Jakobsson, & and Menczer (2007)	**Description and finding:** Authors harvested data about subjects from social networking sites to launch a phishing attack. They found that the context of a phishing attack leads targets to overlook cues that point to deception, making them more vulnerable. **Recommendation:** Use of browser toolbars that alert users to phishing. Extensive educational campaigns about phishing and other security threats, for example, warning students that anyone is susceptible to phishing.
Kumaraguru et al., (2007)	**Description and finding:** authors argue that users often ignore anti-phishing educational materials despite their wide availability. Using an embedded training methodology to train people to avoid phishing, they found that users retained anti-phishing knowledge longer. **Recommendation:** Anti-phishing training should be based on phishing exercises that train users immediately after they fail to recognize a phishing attempt. Training materials should be not sent by email because users tend to ignore them and are not motivated to read the instructions.
Kumaraguru, Sheng, Acquisti, Cranor, & Hong, (2010)	**Description and finding:** authors examined how to educate users about phishing and helping them make better decisions. Their findings identified many challenges for anti-phishing education, including, lack of motivation to learn about security, difficulties of teaching people to identify security threats without increasing their tendency to misjudge legitimate emails for phishing ones. **Recommendation:** Automated defense systems as the first line of defense against phishing attacks. Education as a complementary approach to help people better recognize fraudulent emails and websites.
Kumaraguru et al., (2009)	**Description and finding:** authors examined the long-term retention of training messages and the factors that influence training and phishing susceptibility. They found that users trained with PhishGuru retain knowledge even after 28 days and that additional training reinforces the training effect, thereby reducing the likelihood of people giving information to phishing websites. They also found that training does not decrease users' willingness to click on links in legitimate messages. **Recommendation:** PhishGuru should be used to train users about phishing on a continuous basis.
Mohebzada, El Zarka, BHojani, & Darwish (2012)	**Description and finding:** authors conducted a phishing experiment by sending spoofed emails which appeared to come from a legitimate source to trick the recipients into revealing personal information to a phishing website. They found that lack of awareness about phishing is a reason people submit information to phishing websites. People also ignore warning messages, and do not understand the consequences of falling for a phish. **Recommendation:** education and awareness programs should be designed to combat

	phishing.
Vishwanath, Herath, Chen, Wang, & Rao, (2011)	**Description and finding:** Authors tested a model of how individuals evaluate and process phishing emails. They found that most phishing emails are peripherally processed, and individuals rely on simple cues embedded in the phishing emails when deciding whether an email is phishing or not. **Recommendation:** Individuals should reserve specific times for reading of emails and for responding to them. This increases cognitive effort and reduces likelihood of clicking on a phishing link
Wang et al., (2016)	**Description and finding**: authors examine the role of overconfidence in phishing email detection. Their findings indicate that overconfident individuals exerted less cognitive effort when processing phishing emails. **Recommendation:** recognize sources of overconfidence and devise mechanisms to reduce it. Teach users to reduce overconfidence with self-awareness and formal training. Expose overconfident individuals to tougher training.
Wang, Herath, Chen, Vishwanath, & Rao (2012)	**Description and finding:** authors investigated how individuals process phishing emails and determine whether to respond to them. They found that attention to visceral triggers that stress urgency of response and attention to phishing deception cues, reduce information processing whereas phishing knowledge increases systematic processing. **Recommendation:** Message title and content are not reliable indicators of email quality because phishing emails display high quality designs. Organizations should invest in scam awareness programs, training, or education programs to enhance employee's security knowledge.
Wright et al., (2014)	**Description and finding:** authors applied persuasion and motivation theory to explain why certain influence techniques are dangerous when used in phishing attacks. They found that users process information peripherally and techniques such as liking, social proof, scarcity, and reciprocity, increase the likelihood of complying with phishing emails. **Recommendation:** raise awareness about phishing influence techniques through anti-phishing training programs.
Wright & Marett (2010)	**Description and finding:** authors studied the behavioral factors that may increase a person's susceptibility for complying with phishing. They found that individuals with computer self-efficacy, web experience, and security knowledge and a high perceived suspicion are less likely to comply to phishing emails. **Recommendation:** experience and training are the most effective tools against phishing. People should engage in prolong conversations with email senders to determine their legitimacy.
Wu, Miller, & Garfinkel (2006)	**Description and finding:** authors examined whether toolbars really prevent users from being tricked into providing personal information to phishers. They found that many users failed to pay attention to toolbar warnings even though they were asked to focus on them. Many users do not understand phishing attacks and fail to realize how sophisticated such attacks can be. **Recommendation:** authors recommend active interruptions such as popup windows that can interrupt users who want to submit information to suspicious websites with warnings. Warnings should propose an alternative path for users to complete their tasks.
Yang, Xiong, Chen, Proctor, & Li (2017)	**Description and finding:** authors argued that users can make correct, informed decisions when the reasons for warnings about suspicious sites are conveyed with the warning. In a field experiment, they found that knowledge about phishing improves the effectiveness of phishing warnings and reduces the number of people phished. However, phishing knowledge alone was insufficient. **Recommendation:** authors recommend integrating training in a warning interface and explaining to the user why the warnings are generated.
Zielinska et al., (2014)	**Description and finding:** authors argue that although multiple training measures against phishing have been developed, training that emphasizes phishing consequences and increases users' fear levels have not been developed. They recruited participants through Amazon Mechanical Turk (MTurk). They found that although training improves a users'

	ability to identify phishing emails, it also caused increased false alarms. **Recommendation:** authors recommend focusing on the long-term effects of training to improve knowledge retention for up to one year.

4. Addressing the research questions

RQ 1. Why do people fall for phishing?

Previous phishing research has identified the reasons why people become phishing victims. These reasons (summarized below) are typically modeled as the independent variables/factors for becoming a phishing victim.

1. Overconfidence

According to phishing research, overconfidence represents an important problem for organizations with regards to security violations. Wang et al., (2016) examined the role of overconfidence in phishing and reported that it increases when individuals selectively focus on information that confirms what they already know or suspect about an email. For example, when a phishing email contains familiar attributes, such as familiar sources and familiar business entities, the recipients of the phishing email tend to focus on the familiar attributes and ignore contradictory information (e.g., incorrect spellings and poor grammar). This increases their likelihood of becoming phishing victims. The authors reported that overconfidence is an optimistic disposition that is more common among the educated. IT professionals and employees who have benefitted from security education may be misguided by their knowledge and training to take excessive risks while believing that they can always successfully handle future phishing

threats (Wang et al., 2016; Goel et al., 2017). Overconfident individuals overestimate their abilities (Moody, Galletta, Walker, & Dunn, 2011).

2. **A trusting disposition**

Phishing scholars have also reported that individuals with a highly trusting disposition are more susceptible to phishing than individuals who are suspicious of humanity (Wright & Marett, 2010). In human interactions, there is an expectation that the trusted party has a moral responsibility toward the trusting party (Hertzum, 2002). Specifically, trusting individuals tend to demonstrate a willingness to take risks and to be vulnerable in situations where meaningful incentives are at stake (Mayer, Davis, & Schoorman, 1995). Notwithstanding, trust depends on many situational factors that involve the trusting party assessing whether the other party possesses the required knowledge and skills (Hertzum, 2002). Phishers often meet these requirements by sending phishing emails that contain relevant information. Such emails require a recipients' urgent attention and will supposedly cost them if the emails are ignored. In some cases, the phishers patiently develop and nurture a personal rapport with an employee through multiple communications while impersonating someone in authority, a contractor, or someone from IT management.

Researchers have found that phishing emails use influencing techniques, such as scarcity, consistency, social proof, and reciprocity to dissuade the recipients from engaging in systematic information processing while encouraging more peripheral information processing (Wright et al. 2014). Typically, trust is an important component of electronic communication as it increases the likelihood of sharing information and exploring new mutually beneficial business arrangements (Ratnasingham, 1998). The problem for organizations with trusting employees is accentuated by the commonplace use of familiar business entities, names, logos, and slogans in phishing attacks.

3. Peripheral information processing

In phishing research, peripheral processing involves attending to information selectively, often ignoring important cues that can reveal an email as a phishing attempt (Goel et al., 2017; Wright & Marett, 2014). It is a major reason people fall for phishing emails. Phishing emails that are contextualized and require urgent responses often compel people to make quick and intuitive judgments that lack careful deliberation (Goel et al., 2017). Many organizations are training their employees about phishing and what they should do when they encounter one (Kumaraguru et al., 2010). However, the persuasiveness of phishing emails, overconfidence, and curiosity, means that individuals continue to ignore such security recommendations inadvertently or deliberately. Because deceptive cues are always involved in a phishing attack, it is likely that an element of carelessness is also a cause of phishing (Jakobsson, 2007). Viswanath et al. (2011) reported that habitual email use also explains why people fall victims to phishing.

4. Habit

According to phishing research, a habit of clicking on emails increases the likelihood of becoming a phishing victim (Vishwanath et al., 2011). Habit is a routine behavior and habitual users perform actions because they are accustomed to acting in that way (Vance, Siponen, & Pahnila, 2012). Habit develops overtime, through repetitive action and the mind no longer exerts many resources to process the task (LaRose, Lin, & Eastin, 2003). Habitual email use increases phishing victimization because habitual users fail to actively attend to the information and instead, they either automatically or subconsciously respond to relevant emails without systematically processing the emails in detail (Vishwanath et al., 2011).

RQ 2. What are the existing recommendations against phishing?

The threat of security violation is constant because there are multiple sources for security breaches. For example, the network system of an organization breached through a phishing attack can be used to also attack its partners relying on that network. Scholars have made several suggestions aimed at reducing IS security breaches. Many organizations are using technology to improve security, by automating processes such as patch management and antivirus updates, thereby reducing task knowledge and its accompanying burden on their employees (Herath & Rao, 2009). Organizations have also developed security policies for tasks including the appropriate use of the computer and network resources and appropriate password habits. However, researchers have also noted that despite the benefits from using security technologies and practices, information security cannot be achieved through technological tools alone (Herath & Rao, 2009). To address these security problems, researchers have proposed additional measures for reducing the risks of individuals becoming phishing victims. These are discussed below.

1. **Security education and awareness training**

In general, researchers and practitioners consider anti-phishing security education, training and awareness to be the optimal approach to avoid becoming a phishing victim. Organizations are advised to continuously organize security awareness programs to remind their employees that phishing emails are a serious information threat (Pattinson et al., 2012). Many studies have reported that users generally find phishing education delivered through books, papers, and articles boring because they do not receive immediate feedback (Dodge et al., 2007). Similarly, researchers recommend against sending anti-phishing materials via email because users are not often motivated to read the instructions (Kumaragu et al., 2007). Therefore, some researchers recommend interventions based on learning science (Kumaraguru et al., 2010).

Kumaraguru et al., (2010) used learning science to propose an embedded approach that emphasizes learning by doing; more precisely, employees are sent phishing emails in their email accounts and those who fall for them receive immediate training. Although the researchers reported that knowledge retention increases when the users receive immediate feedback, they also recommend regular training to enable the users to identify other types of phishing email (Dodge et al., 2007; Kumaraguru et al., 2007). Further, drawing on learning science and studies done on eye tracking, researchers have developed anti-phishing games that are considered more effective than traditional classroom-based approaches (Archchillage et al., 2016). Regardless, anti-phishing training and awareness increases people's computer self-efficacy, web experience, security knowledge, and makes people more suspicious of email requests (Wright et al. 2010). Sheng et al., (2010) reported that education and training reduced the user's tendency to enter information into phishing webpages by 40% percent. Security education is generally considered an effective anti-phishing tool because phishers use phishing to prey on the naïve and vulnerable for their personal information (Wright et al., 2010); researchers view education as an important means of motivating individuals to process information more systematically (Wright et al., 2014).

2. Training users to systematically process information in emails

Many phishing studies have reported that people become phishing victims because they rely on System 1 thinking to process information peripherally (Wright et al., 2014; Wang et al., 2012). Wright et al. (2014) reported that phishing emails deceive people through influencing techniques that include consistency, scarcity, authority and urgency. These techniques induce people to make decision errors by triggering a response that selectively focuses on the portions of phishing emails that emphasize urgency. The urgency cues reduce systematic processing when the

phishing email is contextualized or relevant to the recipient (Goel et al., 2017). Contextualization motivates phishing email recipients to ignore any elements that reveal deception, such as spelling and grammar errors (Vishwanath et al., 2011). Therefore, researchers recommend that anti-phishing programs should train people to resist the triggers that reduce systematic information processing (Wang et al., 2012).

3. Better website designs and automating security

Because phishers use spoof websites to deceive people into submitting personal and sensitive information, researchers have suggested that phishing education should also include training people to identify legitimate websites from phishing ones (Wu et al., 2006). While training programs should teach people to understand the structure of URLs organizations should make their URL bars more user-friendly (Alsharnouby et al., 2015; Wu et al., 2006). Because legitimate websites that use different domains for different sections of their website are confusing for users, they are often ignored. Therefore, if URLs are to be a reliable aid in detecting phishing, organizations can make their domain names an effective security tool by ensuring they are visually distinct and uniform (Alsharnouby et al., 2015). However, because people consistently fail to accurately detect phishing websites, researchers also recommend that organizations automate as much as possible (Wu et al., 2006; Alsharnouby, 2015), while using education as a second line of defense (Kumaraguru et al., 2010).

In summary, previous phishing research recommends security education, training, and awareness programs to motivate individuals to process emails more systematically. Previous research also suggests that organizations should automate as much as possible because security education is still not very effective. Findings in other areas of IS security violations (Puhakainen & Ahonen,

2006), suggest that individuals who have been exposed to security training fail to perform specified security behaviors. This leads to the third question.

RQ 3: Why are the existing recommendations not very effective?

Researchers assumed that using security education and awareness training to teach people to avoid becoming phishing victims would be effective. However, past research has reported that this has not been very effective; the extant training and education programs are not yielding the intended results. Many studies have reported that users who have received anti-phishing training, whether they are cadets in the US academy (Dodge et al., 2007) or students in US universities (Moody et al., 2011), fail to follow the recommended advice. Wright and Marett (2010) taught university students about phishing and information security for eight weeks. The students were each assigned a "super-secure code" that they were never supposed to disclose to anyone under any circumstances. However, when the students received phishing emails asking for their super-secure codes, the majority complied with the request. While some students gave no reasons for sharing their codes, others thought that the emails appeared legitimate, and they wanted to help management fix a database problem as mentioned in the emails. Similarly, when Dodge et al. (2007) sent phishing emails to the military cadets who had received security training on phishing, the majority also fell for the phishing attack.

Although security education remains the number one recommendation, research for a ten-year period has suggested that it has not been very effective (Alsharnouby et al., 2015). Many anti-phishing recommendations do not specify any target group for the recommendations. For example, although researchers typically collect background information about their study subjects, such as demographics and dispositional and situational characteristics, they often do not

consider this information when proposing anti-phishing recommendations. Consequently, the recommendations adopt a "one-size fits all" approach that does not consider the specific needs of any demographic or group of individuals. This is a generic approach where researchers propose the same anti-phishing recommendations to anyone susceptible to becoming a phishing victim. Researchers are making generic recommendations because they consider that the reasons for falling for a phish are the same. However, by assuming that the same security awareness training programs are applicable to all users who are susceptible to phishing may be simplifying behaviors. When individuals encounter phishing emails, they may have one or more reasons for clicking on a phishing link.

The second reason follows from the first: because recommendations are not targeted to a specific audience, the users must cope with too many recommendations. In a recent study, Goel et al. (2017) acknowledged that phishing has not been very effective, and suggested that the problem may be because there are too many recommendations: "*past training has not been very effective, which we posit may be due to the vast array of techniques of deception and human cognitive limitation to process and absorb them*" (p. 36). The authors collected data from thousands of university students, and examined the differences among their academic majors and how such differences affected their reasons for complying with phishing emails. However, Goel et al. failed to use all the information collected to propose a targeted message to phishing education. Instead, the authors simply stated that: "*creating highly focused and contextualized awareness campaigns targeted to different audiences based on their cognitive biases may improve the impact of the training provided*" (p. 36). With the information they collected, an effective approach, would incorporate the reasons for the differences among the selected majors in making any recommendations. Notwithstanding, the authors' acknowledgement that training should be

contextualized constitutes an improvement when compared to the earlier research. With a few exceptions (e.g., Downs et al., 2006), the previous research does not consider anti-phishing education based on targeted communication.

RQ 4: How can anti-phishing recommendations be more effective?

This question discusses our suggestions for improving anti-phishing recommendations and reducing phishing overall. Phishing recommendations can be made more effective by profiling phishing victims and categorizing them into stages. This means that in addition to their primary research question, researchers studying why people are victimized by phishing victims should consider the following additional question: "Do phishing victims reside in stages?" Stages are theoretical constructs that can be determined either empirically or theoretically (Schwarzer, 2008; Weinstein et al., 1998).

First, this study proposes a prototype for each stage to show how researchers can determine the stages of phishing. Several stage theorists have advanced different means of determining stages (Prochaska & Velicer, 1997; Weinstein et al., 1998). The following properties are common among stage theories: (1) a classification system to define the stages, (2) an ordering of the stages, (3) common barriers to change facing people in the same stage, and (4) different barriers to change facing people in different stages. Stages are theoretical constructs and the requirement for stages can be contextualized to address the problem to be examined. However, when developing a stage theory, not all the properties may be necessary to address the problem under study. Accordingly, in phishing research, the properties that define a stage can be determined as follows:

1. **A system to classify individuals into specific stages**: individuals are assigned to a specific stage because they share similar attributes to others in the same stage. However, significant differences exist between individuals belonging in one stage (e.g., Stage 1) and individuals belonging in another stage (e.g., Stage 2).
2. **Progress along the stages:** As individuals belonging to a stage improve their security knowledge and experience, they may progress to the next higher stage. However, progress along the stages does not have to be sequential.
3. **Similar barriers:** individuals grouped into a stage are expected to experience similar problems or security challenges and that similar interventions can be designed to help them.

5. The Stages of Phishing Victims

The stages of phishing victims can be determined by focusing on the reasons that victims give for complying with phishing emails. Stages would not be needed if the reasons people click on phishing links were the same because a similar intervention could be used for everyone. However, the concept of stages is justified in behavioral phishing research by the fact that people have different reasons for clicking on phishing links and these reasons change. Stage theories construe change as temporal, indicating phenomena occurring over time (Prochaska & Velicer, 1997).

Although previous phishing research does not examine the presence or absence of stages, some findings indicate that victims may be residing in qualitatively different stages. The information for categorizing individuals into stages may also come from the background information about the subjects. Additional information about their reasons for clicking on phishing links may be

obtained through follow-up interviews. This may lead the researchers to classifying individuals as residing in two, three, or more stages. Thus, it may be that individuals in Stage 1 have received little or no security training; individuals in Stage 2 have some security training and individuals in Stage 3 are advanced users with advanced security knowledge.

Furthermore, when the subjects with different security experiences and online behaviors are subjected to similar phishing experiments, the findings are contradictory. For instance, on the role of computer self-efficacy in phishing, Moody et al. (2011) and Wang et al. (2016) reported that individuals high in computer self-efficacy are susceptible to phishing because they are overconfident in their abilities. In contrast, others (e.g., Wright & Marett, 2014) reported that high self-efficacy reduces the risks of phishing susceptibility. One plausible explanation is that the subjects are in qualitatively different stages, possess different skills, knowledge, and have different reasons for complying with phishing emails.

A key advantage of a stage-based approach is that the phishing victims are categorized or grouped based on whether they possess different or similar characteristics (Weinstein et al., 1998). However, accurately placing users in the correct stage may be a complicated task due to the numerous factors that may influence their phishing behaviors. Regardless, profiling users into stages will have a huge impact on how the anti-phishing messages are developed and delivered.

Anti-phishing recommendations should use targeted communication. Stage theorists suggest that individuals located at a specific stage should be identified and targeted with messages that can most effectively change their behaviors (Weinstein et al., 1998). This is because individuals in different stages have different characteristics and members in a specific stage share similar attributes. However, the extant phishing research rarely offers messages that target a specific audience. Consequently, individuals are exposed to many recommendations. In contrast, an

approach based on targeted communication would consider the characteristics of users in the different stages. If the message is effective and, for example, some individuals in Stage 1 (naïve users) progress to a higher stage (Stage 2), it becomes easier to identify the factors or attributes that contribute to progress and to understand the barriers that prevent other people from moving from one stage (e.g., Stage 1) to another (e.g., Stage 2). An ineffective message may lead researchers and practitioners to consider new sets of questions: is security education inadequate or are some people simply careless? Do such individuals require more frequent security training? With targeted communication, anti-phishing education will consider what individuals already know and what they don't know, and what their online behaviors involve. By considering a subset of individuals (a stage of individuals), their online behaviors or activities, their existing security knowledge, and computer self-efficacy, researchers and practitioners can develop messages that are more effective for the individuals in one stage and that are maybe useless or incomprehensible to individuals in a different stage. For example, whereas generic messages such as be careful online, don't click on emails from a bank might be useful to a naïve computer user in Stage 1, the message might be useless to more advanced users in Stage 2 or Stage 3. With the primary data, and knowledge of who their subjects are, and why they acted as they did, the researchers are able to provide more actionable recommendations. Therefore, it is not enough that researchers simply state that phishing might be more effective when the messages are contextualized (Goel et al., 2017).

Finally, as individuals are exposed to anti-phishing security education and training, researchers and practitioners should consider that their reasons for clicking on phishing links are not static and will likely change over time. Previous phishing research does not consider that people's reasons for clicking on phishing may change. Consequently, individuals who at one time clicked

on a phishing link because they lacked the requisite security knowledge, after receiving security training, may click on a link because they are overconfident in their abilities.

Therefore, to determine the stages of phishing with empirical data, researchers should focus on the reasons for people's behaviors when they interacted with the phishing emails that deceived them. Based on the findings from previous phishing research, three stages of phishing were identified. The identified stages are only meant to serve as examples of how researchers can determine or develop their own stages in behavioral phishing research.

5.1. Demonstrating how researchers can propose stages of phishing victims and targeted anti-phishing recommendations

Stage 1:

This stage comprises individuals who use System 1 thinking to process information (Wright et al. 2014). Such individuals may have no previous security experiences and may be unaware that their online behaviors pose a security risk to them. They are the naïve users that many researchers have talked about in the phishing literature (Downs et al., 2006; Jakobsson, 2007). Downs et al., (2006) specifically studied naïve computer users. To qualify for their study, the authors ensured that their subjects were "*sufficiently inexperienced in computer security*" (p. 6). They disqualified people from participating in the study if they had adjusted their security preferences on their computer or had helped another person with a computer security problem (e.g., scanning for viruses), thereby ensuring that only "*a particularly security-naïve subset of the general population*" (p. 6) were eligible for their study. Assuming that individuals cannot be any more naïve about computer security, the subjects in the Downs et al. study were probably

located in the lowest stage of a phishing stage model. Such users are easily influenced by urgency cues in phishing emails that emphasize threats or rewards. Accordingly, for Stage 1 users, the goal of anti-phishing programs should be to develop an awareness about security risks. They should also be informed that their online behaviors can present a major security risks.

Stage 2:

These are individuals who have been exposed to anti-phishing education programs. However, they do not often extrapolate to identify and avoid phishing attempts that they are unfamiliar with. Such individuals require continuous security training and awareness (Dodge et al., 2007). Stage 2 users need more than a mere reminder about online security risks. Moreover, they should be taught about how to verify the authenticity of a suspicious email. For example, teaching them how to systematically process information and avoid missing information outside their periphery of attention (Dhamija et al., 2006). The goal of anti-phishing programs is to help such users verify the authenticity of a suspicious email by motivating them to focus on the source of the email and other cues that typically suggest deception. In addition, anti-phishing education should also include simulated phishing exercises (Kumaraguru et al., 2007).

Stage 3:

These are individuals who have benefitted from continuous security training and awareness programs and have a high computer self-efficacy. Such individuals systematically process phishing information. However, their advanced security knowledge may also cause them to be overconfident (Wang et al., 2016; Moody et al., 2011). Overconfidence may be their reason for clicking on a phishing link. Because these individuals are already experienced with security

issues, the goal of anti-phishing programs should be to help them engage in protracted conversations ascertain that an email is legitimate and discourage complacency.

6. Limitations

This study relied on published research on phishing victims. In most previous phishing studies, the subjects had been informed about the purpose of the study (e.g., Moody et al. 2011, Wright & Marett 2010). (Parsons, McCormac, Pattinson, Butavicius, & Jerram, 2015) conducted a study in which over half of their subjects were informed about the purpose of the study. They reported that subjects that were informed about the purpose of the study, were significantly better at discriminating between phishing and legitimate emails than the uninformed subjects. This highlights the need for caution in interpreting previous phishing research; the different methodologies adopted by researchers may have implications for their findings and their recommendations. Future research can overcome this problem by interviewing actual phishing victims.

Further, our recommendation that phishing researchers categorize phishing victims into stages and develop targeted messages is not based on direct empirical evidence. Nonetheless, evidence from cancer research and health psychology suggest that targeted messaging is efficacious and cost-effective (Prochaska, Velicer, Fava, Rossi, & Tsoh, 2001; Lairson, Newmark, Rakowski, Tiro, & Vernon, 2004). Thus, the impact of targeted messaging in phishing could be quite large.

7. Conclusion

Phishing attacks represent a major form of online identity theft and there is already a large and growing empirical literature on phishing with numerous recommendations to reduce it. Past research on phishing has proposed many recommendations aimed at reducing phishing, including security education, training, and automation. The effectiveness of the education programs often depends on how they are delivered. IS researchers have used many training approaches, such as face-to-face learning, e-learning, computer-based training, and social engineering preventive approaches. However, the extant recommendations are not based on any specific knowledge or understanding of the individuals who fall for phishing emails. Several researchers have reported that extant training and security awareness recommendations have not been very effective. In the current study, the empirical phishing literature was reviewed with a primary focus on the effectiveness of anti-phishing recommendations.

The review found that phishing research primarily uses continuum models to develop theoretical explanations for phishing and to make practical recommendations to reduce it. This study has argued that the continuum approach leads to recommendations that are generic because it does not consider that individuals reside in different stages, have stage-specific reasons for their clicking on phishing links, and will change the reasons for their behaviors over time. In contrast, if the anti-phishing recommendations adopt a stage approach, the researchers will examine any contributory factors to phishing victimization and conduct follow-up to ascertain the reasons why individuals clicked on phishing links. Based on the finding, I have suggested a prototype for how researchers can develop stage theories for phishing victims. Analysis of the previous phishing research also led to identification of three stages for phishing victims. It is suggested that anti-

phishing recommendations should match the needs of individuals in the different stages of phishing that researchers develop.

References

Alnajim, A., & Munro, M. (2009). An evaluation of users' anti-phishing knowledge retention. *Information Management and Engineering, 2009. ICIME'09. International Conference On,* 210-214.

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies, 82*, 69-82.

APWG. (2017, Phishing activity trends report. *Anti-Phishing Working Group,*

Arachchilage, N. A. G., & Cole, M. (2016). Designing a mobile game for home computer users to protect against phishing attacks. *arXiv Preprint arXiv:1602.03929,*

Arachchilage, N. A. G., Tarhini, A., & Love, S. (2015). Designing a mobile game to thwarts malicious IT threats: A phishing threat avoidance perspective. *arXiv Preprint arXiv:1511.07093,*

Dhamija, R., Tygar, D., & Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* 581-590.

DiClemente, C. C., Prochaska, J. O., Fairhurst, S. K., Velicer, W. F., Velasquez, M. M., & Rossi, J. S. (1991). The process of smoking cessation: An analysis of precontemplation, contemplation, and preparation stages of change. *Journal of Consulting and Clinical Psychology, 59*(2), 295.

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

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. *Proceedings of the Second Symposium on Usable Privacy and Security,* 79-90.

Egelman, S., Cranor, L. F., & Hong, J. (2008). You've been warned: An empirical study of the effectiveness of web browser phishing warnings. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* 1065-1074.

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? internet security and human vulnerability. *Journal of the Association for Information Systems, 18*(1), 22.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

Hertzum, M. (2002). The importance of trust in software engineers' assessment and choice of information sources. *Information and Organization, 12*(1), 1-18.

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

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

Jakobsson, M. (2007). The human factor in phishing. *Privacy & Security of Consumer Information, 7*, 1-19.

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University, 33*(2004), 1-26.

Korolov, M. (2015, Report: Average cost per record breached is 58 cents, discovery times are down. *CSOonline,*

Kreuter, M. W., & Wray, R. J. (2003). Tailored and targeted health communication: Strategies for enhancing information relevance. *American Journal of Health Behavior, 27*(1), S227-S232.

Kreuter, M. W., & Skinner, C. S. (2000). Tailoring: What's in a name? *Health Education Research, 15*(1), 1-4.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting people from phishing: The design and evaluation of an embedded training email system. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* 905-914.

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.

Lairson, D. R., Newmark, G. R., Rakowski, W., Tiro, J. A., & Vernon, S. W. (2004). Development costs of a computer-generated tailored intervention. *Evaluation and Program Planning, 27*(2), 161-169.

LaRose, R., Lin, C. A., & Eastin, M. S. (2003). Unregulated internet usage: Addiction, habit, or deficient self-regulation? *Media Psychology, 5*(3), 225-253.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709-734.

Mohebzada, J., El Zarka, A., BHojani, A. H., & Darwish, A. (2012). Phishing in a university community: Two large scale phishing experiments. *Innovations in Information Technology (IIT), 2012 International Conference On,* 249-254.

Moody, G., Galletta, D., Walker, J., & Dunn, B. (2011). Which phish get caught? an exploratory study of individual susceptibility to phishing.

Noar, S. M. (2006). A 10-year retrospective of research in health mass media campaigns: Where do we go from here? *Journal of Health Communication, 11*(1), 21-42.

Noar, S. M., Benac, C. N., & Harris, M. S. (2007). Does tailoring matter? meta-analytic review of tailored print health behavior change interventions. *Psychological Bulletin, 133*(4), 673.

Okoli, C. (2015). A guide to conducting a standalone systematic literature review. *Communications of the Association for Information Systems, 37*(1), 43.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The design of phishing studies: Challenges for researchers. *Computers & Security, 52*, 194-206.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? Information Management & Computer Security, 20(1), 18-28

Prochaska, J. O. (1994). Strong and weak principles for progressing from precontemplation to action on the basis of twelve problem behaviors. *Health Psychology, 13*(1), 47.

Prochaska, J. O., & Velicer, W. F. (1997). The transtheoretical model of health behavior change. *American Journal of Health Promotion, 12*(1), 38-48.

Prochaska, J. O., Velicer, W. F., Fava, J. L., Rossi, J. S., & Tsoh, J. Y. (2001). Evaluating a population-based recruitment approach and a stage-based expert system intervention for smoking cessation. *Addictive Behaviors, 26*(4), 583-602.

Puhakainen, P., & Ahonen, R. (2006). Design theory for information security awareness.

Ratnasingham, P. (1998). The importance of trust in electronic commerce. *Internet Research, 8*(4), 313-321.

Rimal, R. N., & Adkins, A. D. (2003). Using computers to narrowcast health messages: The role of audience segmentation, targeting, and tailoring in health promotion.

Schwarzer, R. (2008). Modeling health behavior change: How to predict and modify the adoption and maintenance of health behaviors. *Applied Psychology, 57*(1), 1-29.

Sutton, S.General description & theoretical background stage theories assume that behavior change involves movement through a sequence of discrete stages, that different variables influence different stage transitions, and that effective interventions need to be matched to stage (sutton.

Tambe Ebot, A. C. (2017). Explaining two forms of internet crime from two perspectives: Toward stage theories for phishing and internet scamming. *Jyväskylä Studies in Computing 259.,*

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(3), 190-198.

Velicer, W. F., & Prochaska, J. O. (2008). Stage and non□stage theories of behavior and behavior change: A comment on schwarzer. *Applied Psychology, 57*(1), 75-83.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576-586.

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *Professional Communication, IEEE Transactions On, 55*(4), 345-362.

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

Weinstein, N. D., Rothman, A. J., & Sutton, S. R. (1998). Stage theories of health behavior: Conceptual and methodological issues. *Health Psychology, 17*(3), 290.

Weinstein, N. D., & Sandman, P. M. (1992). A model of the precaution adoption process: Evidence from home radon testing. *Health Psychology, 11*(3), 170.

Whitehead, D., & Russell, G. (2004). How effective are health education programmes—resistance, reactance, rationality and risk? recommendations for effective practice. *International Journal of Nursing Studies, 41*(2), 163-172.

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. doi:10.1287/isre.2014.0522

Wu, M., Miller, R. C., & Garfinkel, S. L. (2006). Do security toolbars actually prevent phishing attacks? *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* 601-610.

Yang, W., Xiong, A., Chen, J., Proctor, R. W., & Li, N. (2017). Use of phishing training to improve security warning compliance: Evidence from a field experiment. *Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp,* 52-61.

Zhang, W., Luo, X., Burd, S. D., & Seazzu, A. F. (2012). How could i fall for that? exploring phishing victimization with the heuristic-systematic model. *System Science (HICSS), 2012 45th Hawaii International Conference On,* 2374-2380.

Zielinska, O. A., Tembe, R., Hong, K. W., Ge, X., Murphy-Hill, E., & Mayhorn, C. B. (2014). One phish, two phish, how to avoid the internet phish: Analysis of training strategies to detect phishing emails. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, , 58*(1) 1466-1470.