UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

LEARNING NOT TO TAKE THE BAIT: AN EXAMINATION OF TRAINING METHODS AND OVERLEARNING ON PHISHING SUSCEPTIBILITY

A DISSERTATION

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

Degree of

DOCTOR OF PHILOSOPHY

By

CHRISTOPHER NGUYEN
Norman, Oklahoma
2018

LEARNING NOT TO TAKE THE BAIT: AN EXAMINATION OF TRAINING METHODS AND OVERLEARNING ON PHISHING SUSCEPTIBILITY

A DISSERTATION APPROVED FOR THE
DEPARTMENT OF PSYCHOLOGY

BY

_____
Dr. Eric Day, Chair

_____
Dr. Shane Connelly

_____
Dr. Michael Kramer

_____
Dr. Matthew Jensen

_____
Dr. Jorge Mendoza

_____
Dr. Lori Snyder

To my parents Hero Nguyen and Donna Huynh.

Acknowledgements

I have so many people that I would like to acknowledge for helping me reach this milestone. First and foremost, I would like to thank my major professor and mentor Eric Day for his guidance throughout my graduate school career. He has pushed me to become a better researcher and person, and I am honored to have learned from someone who reminds me to pursue all things in life with passion. Second, I would like to thank my committee members Shane Connelly, Michael Kramer, Jorge Mendoza, and Lori Snyder for their unwavering support and continuing to believe in my potential even in the most challenging of times. Third, I would like to thank Alexandra Durcikova, Matthew Jensen, and Ryan Wright for welcoming me with open arms when I joined their grant team and helping me figure out logistics, materials, and everything in between throughout the course of this project. Fourth, I would like to thank Lynnetta Eyachabbe and her team in the OU IT department for partnering with me and making this a project that I am incredibly proud to have put together and excited to share with others. Fifth, I would like to thank Larry Arthur, Murad Moqbel, Shreyasi, and JEB Sheriff for allowing me to incorporate this project in their classes and make this into a meaningful learning opportunity for their students. Sixth, I would like to thank my classmates in the psychology department for their help piloting my materials and providing me with invaluable feedback. Finally, I would like to thank my dearest friends, mentors, brother Tony, sister-in-law Loan, and parents for their unconditional love and support throughout my time at OU. These past 5 years in graduate school have been some of the most trying times in my life, and I am so incredibly grateful to have these people in my life who have encouraged me every step of the way.

Table of Contents

List of Tables

List of Figures

Abstract

As phishing attacks become increasingly common and sophisticated, anti-phishing training must extend beyond teaching individuals about cues and rules associated with phishing. Specifically, training methods that teach individuals effective allocation of time and attentional resources to the nature and context of emails should be examined, as well as strategies for improving skill retention from training. Thus, the present study compared the effectiveness of rule-based and mindfulness training, as well as the influence of overlearning on training, on two tests of skill retention on phishing susceptibility (i.e., email identification tests and mock phishing attack tests). Participants were 453 university undergraduates who received training and practice and then were tested immediately following training using an email identification test. Participants were then sent mock phishing emails 1 week and 8 weeks after training, as well as an additional email identification test 10 weeks after training. Results showed that individuals who received mindfulness training were significantly better at discriminating between legitimate and phishing emails, less susceptible to phishing attacks, and more cautious of phishing compared to those who received rule-based training. However, the discriminability effect of mindfulness training was subject to a similar rate of skill decay as rule-based training. Although training did not differ as a function of overlearning, individuals who received 100% overlearning were significantly less susceptible to phishing attacks and more cautious of phishing compared to those who did not receive overlearning. Results are discussed regarding implications for implementing effective anti-phishing training to protect individuals and their respective organizations and institutions.

Introduction

According to a 2016 report by the Federal Bureau of Investigation (McCabe, 2016), successful phishing attacks have increased by 270% since January 2015, which has resulted in an estimated 2.3 billion dollars in annual losses related to fraud, theft, damages to reputation, regulatory violations, and loss of intellectual property. To help combat these attacks, several countermeasures have been suggested to assist organizations and individuals in defending themselves, some of which include preventing messages from reaching users through email filters and website blockings, providing better Web interfaces and tools that warn users of suspicious websites, and training users on how to identify phishing emails and websites (Hong, 2012; Kumaraguru et al., 2007a). Although the first two strategies are ideal for protecting users against phishing attacks as a first line of defense, these technological mechanisms are not always foolproof and can be overcome as phishers become more sophisticated in their attack methods. If these attacks manage to bypass automated anti-phishing tools or systems in place and reach individuals' email inboxes, it is ultimately up to individuals to make the decision as to how they will respond. Thus, it is imperative to educate users on the dangers of phishing attacks and how to avoid the negative consequences.

Research has shown that anti-phishing training can increase individuals' capability to identify phishing emails and can reduce their susceptibility to phishing (Karumbaiah, Wright, Durcikova, & Jensen, 2016; Kumaraguru et al., 2007b, 2010; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010). However, the majority of previous anti-phishing training methods have focused on educating individuals on specific cues or signals associated with phishing emails through a rule-based approach,

which may become obsolete as phishing attacks evolve. Relying upon a fixed set of guidelines may not be effective across all contexts and may still leave individuals susceptible to phishing attacks because emails are not critically evaluated and done so out of habit (Vishwanath, Herath, Chen, Wang, & Rao, 2011). Thus, there is a need to examine alternative anti-phishing training methods that train individuals to allocate adequate attention and time to their emails and the context in which they are received.

In addition, few studies have examined the extent to which the skills trained during anti-phishing training are retained over an extended period of time, with most studies examining retention intervals that are less than 1 month. Although it is fairly established that skill retention decreases as time increases (Arthur, Bennett, Stanush, & McNelly, 1998; Wang, Day, Kowollik, Schuelke, & Hughes, 2013), the phishing literature has not thoroughly investigated the rate in which learning from anti-phishing training decays across time and the point in which these training effects diminish. Because constant refresher courses cost organizations time and money, it is necessary that anti-phishing training programs promote learning that is retained for longer periods of time. In this vein, overlearning has been found to be an effective training strategy in increasing retention by providing practice opportunities for individuals that go beyond the point of initial learning (Driskell, Willis, & Copper, 1992). Even so, studies of overlearning have generally found that these benefits quickly diminish over time and are only beneficial for short-term retention. However, given that the majority of overlearning research involves laboratory studies with relatively simple tasks (e.g., verbal recall tasks) and short retention intervals, it is difficult to make clear conclusions

about retention rates of overlearning on training material that is more relevant and practical to real-world situations.

Thus, there were two goals of the present study. First, I was interested in comparing the effectiveness of two anti-phishing training methods: rule-based training and mindfulness training. In contrast to rule-based training that has constituted the majority of anti-phishing training, anti-phishing training that incorporates components from mindfulness training may be particularly beneficial in helping individuals identify phishing emails (Baer, Smith, & Allen, 2004; Brown, Ryan, & Creswell, 2007; Jensen, Dinger, Wright, & Thatcher, 2017). In the context of phishing, mindfulness training teaches individuals to devote their attention and effort to the context in which the messages are received. By first forestalling judgment and then reflecting upon the underlying requests or motives associated with email messages, individuals can make more careful and detailed evaluations that could prevent them from falling for a phishing attack. Although preliminary research on mindfulness training related to phishing has shown promising results in reducing phishing susceptibility, further research is needed to examine its effectiveness in terms of long-term retention (Jensen et al., 2017). For the present study, to evaluate training effectiveness, skill retention was measured not only in regards to performance on explicit email identification tests at the conclusion of training (i.e., maximal performance) but also on tests of vulnerability to mock phishing attacks outside the training environment (i.e., typical performance). In general, when left to their own accord, individuals are much more vulnerable to phishing when they are in their everyday environments. Thus, assessing skill retention through these two types of tests provided a clearer picture of how individuals may differ

in their capability to detect phishing in a more controlled setting versus a real-world setting.

Second, I was interested in examining the influence of overlearning on these two types of anti-phishing training in relation to skill retention. To my knowledge, there have been no studies that have examined overlearning through the lens of anti-phishing training, let alone compared the effectiveness of overlearning on different training methods within the same study. Although overlearning should result in better skill retention in identifying and being less susceptible to phishing emails, it may also result in more automatic processing of messages and consequently less generalizability. This may be detrimental in the context of phishing because evaluating email messages requires conscious effort as no two phishing emails are identical. In other words, as individuals become more familiar and receive more exposure to phishing emails, evaluating these messages may become habitual and done in a thoughtless manner. Thus, examining overlearning in the context of anti-phishing training will provide insight as to whether it would be beneficial in protecting individuals in the long term.

Phishing

According to the Anti-Phishing Working Group, phishing is defined as "a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials" (APWG, 2017; p. 2). Social engineering refers to using influence and persuasion tactics to deceive individuals into revealing confidential information on counterfeit websites, whereas technical subterfuge refers to planting malware onto individuals' computers and systems to steal their information directly (APWG, 2017; Mitnick & Simon, 2002).

Phishing attacks are most commonly initiated through email but may also be conducted through instant messaging or online games. Over the course of 12 years, phishing has increased by an overwhelming 5,753%, with an average of 92,564 phishing attacks per month (APWG, 2017). In this vein, studies have shown that individuals are generally very susceptible to phishing attacks. Individuals were often unable to distinguish between legitimate and phishing websites between 40% and 80% of the time (Abbasi, Zahedi, & Chen, 2012; Dhamija, Tygar, & Herst, 2006; Grazioli and Jarvenpaa, 2000; Herzberg and Jbara, 2008). In addition, over 70% of participants engaged with a phishing website by making purchases and providing sensitive information (Grazioli and Jarvenpaa, 2000; Jagatic, Johnson, Jakobsson, & Menczer, 2007). Thus, without any technological decision-making aids or training available prior to encountering these attacks, individuals are at serious risk of falling for phishing attacks.

Phishing attacks consist of three major phases: the bait (also referred to as lure), the hook, and the catch (Hong, 2012; Myers, 2007). In the bait phase, phishers send users a seemingly legitimate email message that requires their attention. These email messages are often distributed to a large number of individuals with the hopes that a small subset of recipients will fall victim to their attack. The most common requests ask users to click on a Uniform Resource Locator (URL) link embedded in the email message, which redirects them to a website that is controlled by the phisher and used to obtain confidential information from users. Phishers may also utilize other methods of attack such as asking users to open or download an attachment that contains malware or reply to an email with sensitive or confidential information. In the hook phase, users take action on the email by either clicking on the link, downloading the attachment, or

replying to the email. When users click on links, they are redirected to a website that imitates the appearance of the entity being falsely portrayed. For example, if a phisher is attempting to steal bank account information, the layout of the phishing website may look very similar, if not identical, to the actual banking website to convince users of its legitimacy. Finally, in the catch phase, phishers make use of the information they collect from their victims by monetizing the stolen information through activities such as fraud or identity theft. Depending on what the phishers are targeting, users may not be aware that their information has been compromised until an extended period of time has passed.

Phishing is often referred to as a type of semantic attack, which are computer-based attacks that take advantage of the way in which humans interact with computers and interpret messages (Downs, Holbrook, & Cranor, 2006). Thus, phishers rely upon different technical and social tactics to make their emails more credible and persuade users to comply to their requests. Commonly used technical tactics include using legitimate trademarks, logos, and images to convince users that the email sender comes from the actual party or institution, spoofing emails (e.g., forging sender email addresses to conceal the identity of the phisher), and hiding, encoding, and matching links to make the phishing websites appear official and legitimate (Myers, 2007). By mimicking the content and layout of legitimate emails and websites, phishers aim to not raise suspicion in users.

In addition to making emails and phishing websites appear more legitimate, phishers also utilize social engineering tactics to make users more willing and enthusiastic about providing their information. Specifically, phishers use a variety of

influence techniques, some of which include liking, reciprocity, social proof, consistency, authority, and scarcity (Cialdini, 2009; Wright, Jensen, Thatcher, Dinger, & Marett, 2014). Liking refers to gaining compliance through attempts of earning recipients' trust or friendship through praising or emphasizing similarities. Reciprocity refers to making recipients believe they need to repay or owe a favor to the sender in exchange for any services the senders are falsely providing. Social proof refers to making recipients believe that others have already performed the requested action, which is indicated to be the "correct" behavior or response. Consistency refers to taking advantage of individuals' desire to maintain consistency in their actions through describing a false prior commitment made by recipients and then making a request that is consistent with the commitment. Authority refers to referencing or impersonating figures of higher experience, knowledge, or power with hopes that recipients will obey their requests. Scarcity refers to creating a sense of urgency and the illusion that recipients will lose resources if they do not take action. Because these influence techniques are not mutually exclusive, phishers often use them in conjunction with one another. In addition, these social tactics are often used in combination with technical tactics to reinforce the legitimacy of the emails.

Combating Phishing Attacks

In general, three main strategies have been suggested to help users and organizations protect themselves from phishing attacks (Hong, 2012; Kumaraguru et al., 2007a). First, phishing attacks can be prevented from even reaching users. For example, filtering phishing emails, blocking fake websites, and forcibly taking down phishing websites essentially make phishing non-existent to the user by removing any potential

threats before they appear to the user. Second, phishing attacks can be combatted by providing users with better interfaces for their Web browsers and email clients. For example, more advanced warning notifications and identification markers on legitimate websites can help users detect phishing attacks more easily. In addition, more advanced login systems that require multiple forms of user identification make it more difficult for phishers to hack into these systems.

Although these two strategies provide an effective first line of defense, they are only effective if the technology is error-free and users accept the recommendations made by the warning systems. However, studies have shown that these instances are often not the case. For example, Zhang, Egelman, Cranor, and Hong (2006) evaluated the performance of 10 popular anti-phishing tools in detecting 200 verified phishing URLs and found that only one tool was able to identify more than 90% of the URLs correctly. This tool, however, also incorrectly identified 42% of legitimate URLs as phishing URLs. In addition, Abbasi, Zahedi, and Kaza (2012) found that despite being provided an anti-phishing tool that was 90% accurate, individuals still ignored warnings and went against anti-phishing tool recommendations by engaging with phishing websites 21% to 25% of the time.

It is also important to remember that as anti-phishing technology continues to advance, phishing attacks are also advancing. In other words, phishers are learning ways to override current systems and outsmart users through more advanced attack methods. For example, personalized phishing attacks known as spear phishing are particularly difficult to detect (Hong, 2012; Myers, 2007). Instead of mass distributing phishing emails with the hopes that some individuals will fall for the bait, spear

phishing takes into account users' contexts when creating messages, such as only sending bank-related phishing emails to users that have accounts with the referenced bank.

The examples above demonstrate the need for alternative anti-phishing strategies because an overreliance on these technology-based strategies may ultimately be detrimental to users and leave them more vulnerable to phishing attacks. Thus, the third strategy for combating phishing attacks involves training users about what phishing is and how to identify phishing emails. Educating individuals about security in general, however, is a difficult task. In fact, some security experts have argued that user education does not work and is a waste of time and money because individuals are not motivated to read about security and do not take the necessary time to educate themselves (Evers, 2006; Nielsen, 2004). For example, sending security notices alone are not an effective method for educating individuals about the dangers of phishing and other types of semantic attacks because individuals are often overconfident in their capability to protect themselves from these types of attacks; thus, they disregard any security-related information because it is repetitive or already known (Kumaraguru et al., 2007b). In addition, security is often a secondary task for most individuals. For example, individuals may be solely concerned with completing a task (e.g., checking and responding to emails) and not the risks that are associated while working on the task. Challenges also arise where user education may make individuals overly cautious when opening and acting upon their emails, making them more likely to mistake non-threats as threats (e.g., making false positives) that could negatively impact work productivity (Kumaraguru et al., 2010; Sheng et al., 2010).

Despite these arguments, user security education remains an important component of combating against phishing attacks because "as technology increases and becomes more prevalent, the human factor remains the most viable target for would-be attackers" (Purkait, 2012; p. 402). Wright and Marett (2010) found that individuals who are lower on experiential factors such as computer self-efficacy, Web experience, and security knowledge are more susceptible to phishing attacks and conclude that "experience and training appear to be the most effective tools for guarding against phishing" (p. 289). In addition, anti-phishing training may be especially important for individuals between the ages of 18 to 25, who have been found to be the most vulnerable age group due to their lower levels of formal education, higher risk propensity, and less exposure to training materials (Kumaraguru et al., 2009; Sheng et al., 2010). Thus, anti-phishing training is becoming a necessity for high school and college students, particularly those who are entering the workforce and are likely to encounter more frequent phishing emails that can be detrimental to both themselves and their respective organizations.

Anti-Phishing Training

In general, research has shown that anti-phishing training can be effective in reducing phishing susceptibility and helping individuals distinguish between legitimate and phishing emails. For example, Sheng et al. (2007) designed an online game called Anti-Phishing Phil to train individuals on how to identify phishing URLs, search for cues in web browsers, and use search engines to find legitimate websites. Their findings showed that compared to those who were asked to read anti-phishing training materials from existing online resources, individuals who played Anti-Phishing Phil were

significantly better at distinguishing legitimate websites from phishing websites on a criterion task (i.e., website identification task) completed immediately after training. Karumbaiah et al. (2016) found that providing individuals with general video training regarding how to identify phishing messages led to a 44% reduction in individuals' likelihood to click on links embedded in phishing emails on a criterion task (i.e., hypothetical email management task) completed 10 days after training. In addition, Kumaraguru et al. (2007b) designed an embedded anti-phishing training system called PhishGuru that sends fake phishing emails to test individuals and provides immediate training if individuals fall for a phishing email by clicking on a link. Compared to individuals who were emailed phishing information separately to read, individuals who received embedded training had greater motivation to learn and were better at identifying phishing emails both similar and different from the ones presented during training 1 week from the conclusion of training. Sheng et al. (2010) evaluated the effectiveness of these various anti-phishing training materials (e.g., Anti-Phishing Phil, PhishGuru, and web-based training materials) and found that these materials led to a 40% reduction in individuals' tendencies to enter their personal information into phishing websites on a criterion task (i.e., hypothetical email roleplay task) completed immediately after training. However, despite this reduction after training, 28% of individuals still fell for the phishing emails during the roleplay task, which implies the need for other types of anti-phishing training methods.

Rule-Based Training

As a whole, the majority of existing anti-phishing training methods incorporate what can be referred to as rule-based training (Jensen et al., 2017). Rule-based training

teaches individuals how to apply a set of specific guidelines when evaluating emails, such as not clicking on embedded email links from unknown senders or not replying to emails that request confidential information. In addition, rule-based training teaches individuals about specific cues that are likely to allude to a message being phishing, such as requests for urgent action or suspicious URLs (Downs et al., 2006). Although having a list of predetermined guidelines to follow and cues to be on the look out for can help individuals recognize phishing emails more quickly and more effectively, rule-based training works under the assumption that all phishing emails are similar and do not change over time. As phishing attacks evolve and phishers begin developing messages that are much more complex, the same rules and cues once established in the past may become obsolete, limiting the effectiveness of this type of training. For example, spear phishing deviates from the recommendation of not responding to unknown senders by sending individuals customized email messages that appear to come from reputable and known senders (Downs et al., 2006; Myers, 2007).

In addition, these issues are compounded as the rules and cues learned are consistently used and reinforced into an email management routine. By teaching individuals to rely upon simple rules and cues, rule-based training promotes the use of peripheral route processing (also known as System 1 thinking) when evaluating emails, which will likely lead to decisions that are made quickly and carelessly (Petty & Cacioppo, 1986; Stanovich & West, 2000; Vishwanath et al., 2011). By not critically evaluating emails and doing so out of habit, users are much more vulnerable to phishing attacks. In this vein, some phishing influence tactics (e.g., liking, scarcity, social proof,

reciprocity) are especially effective because they exploit users' tendencies to process emails automatically (Wright et al., 2014).

Mindfulness Training

As an alternative to rule-based training, individuals need to be trained to evaluate emails through central route processing (also known as System 2 thinking), which involves the deliberate and conscious evaluation of information (Petty & Cacioppo, 1986; Stanovich & West, 2000). By allocating the necessary time and attention to critically evaluating emails, individuals should be able to better protect themselves from phishing attacks. In this vein, Wright et al. (2014) recommended that future researchers should "investigate methods for encouraging System 2 evaluation, especially when processing requests for private information" (p. 396). Accordingly, anti-phishing training methods that incorporate elements from mindfulness training may be particularly useful for reducing phishing susceptibility.

Mindfulness is defined as "a receptive attention to and awareness of present events and experience" (Brown et al., 2007; p. 212). Although known for its relevance in the clinical psychology literature in treating individuals with behavioral or emotional disorders, these concepts and skills taught in mindfulness training have also been applied to other contexts (e.g., the workplace) to help individuals with their physical and mental well-being (Baer, 2003; Grossman, Niemann, Schmidt, & Walach, 2004; Hulsheger, Alberts, Feinholdt, & Lang, 2012). Baer et al. (2004) outline four skills that are central to mindfulness training: 1) observing; 2) describing; 3) acting with awareness; and 4) accepting (or allowing) without judgment. Observing refers to being present-oriented by noticing and paying attention to surrounding stimuli. Describing

refers to applying non-judgmental labels to observations. Acting with awareness refers to engaging in an activity with undivided attention and focusing on one specific thing at a time. Accepting without judgment refers to being non-evaluative of one's present experience or not responding to a situation through an automatic, impulsive manner.

Using these components of mindfulness training, Jensen et al. (2017) applied mindfulness to the context of anti-phishing training to help individuals better allocate and direct their attention to the evaluation of emails through several steps. First, individuals are taught to attend to the context in which they receive emails. By taking a broader perspective and examining the overall purpose and consequences of the email, rather than the specific content, individuals can get a better understanding of how to approach the situation. In this vein, individuals may be so concerned with quickly fulfilling the request made in the email that they do not recognize that the request itself may be unusual. Second, individuals are taught to fully engage and direct their attention to evaluating emails. By consciously putting in effort to reading and understanding emails, individuals can be more cautious to suspicious requests, particularly during time constraints when quick information processing is likely to occur. Finally, individuals are taught to withhold any judgments of emails until they have gathered sufficient evidence on how to respond. Instead of immediately labeling an email as either legitimate or phishing, individuals should take it upon themselves to investigate the situation further and even consider getting confirmation from a trusted third party. As a preliminary investigation, Jensen et al. (2017) compared the effectiveness of rule-based training and mindfulness training and found that 7.5% of individuals who received mindfulness training responded to a mock phishing attack 10 days after training,

compared to 13.4% of individuals who received rule-based training (p = .04). Overall, training individuals to be more mindful and conscious in their email evaluation appears to be an important strategy for protecting individuals from phishing attacks, and further research is needed to examine the effectiveness of mindfulness training over a longer period of time.

Overlearning

Although previous studies have demonstrated the effectiveness of anti-phishing training, very few studies have examined how the knowledge and skills gained during training are retained over time. In addition, the studies that have examined skill retention in the phishing context (e.g., Alnajim & Munro, 2009; Kumaraguru et al., 2007b; Kumaraguru et al., 2009; Mayhorn & Nyeste, 2012) have only included short retention intervals that are less than 1 month. Thus, more research is needed that examines how learning from anti-phishing training decays over time and what training methods can help individuals retain these skills over longer periods of time. To this end, overlearning may be a particularly useful training strategy to improve skill retention.

Overlearning is defined as "the deliberate overtraining of a task past a set criterion" (Driskell, Willis, & Copper, 1992, p. 615). Overlearning differs from distributed practice such that the continuation of practice occurs immediately after reaching the initial level of learning and is not delayed until a subsequent learning session. Overlearning can benefit retention through several mechanisms, some of which include strengthening the bonds between stimulus and response, reducing cognitive demand by enhancing automaticity, and providing trainees with further practice and feedback on the correctness of responses (Arthur et al., 1998; Wang et al., 2013).

Additionally, individuals who overlearn tasks may also be more resistant to stress-related effects (e.g., narrowed attention) during performance because their tasks become automated and require less active attentional capacity (Driskell & Johnston, 1998). Researchers (e.g., Rohrer et al. 2005; Schendel & Hagman, 1982) have also noted the importance of overlearning when there are severe consequences from forgetting and incorrectly performing a task, particularly those that are infrequently practiced and used only in emergency or crisis situations.

In general, research has consistently shown that overlearning is an effective training technique for retention and that "the importance of continuing practice beyond the point in time where some…criterion is reached cannot be overemphasized" (Fitts, 1965, p. 195). Driskell et al.'s (1992) meta-analytic results indicated a moderate effect of overlearning on retention, with greater degrees of overlearning resulting in greater retention. The authors concluded that with even just 50% overlearning, individuals can expect small improvements in retention. However, the degree of overlearning that is needed may ultimately depend on the type of task being performed. For example, Schendel and Hagman (1982) found that 100% overlearning was optimal for retention on a task involving the assembly of a machine gun, whereas Krueger (1930) found that retention benefits were no longer evident once overlearning exceeded 150% on a maze tracing task. Despite these disagreements, it is well-established that those who receive overlearning will have greater retention compared to those who do not receive overlearning (Krueger, 1929; Juola, 1967; Melnick, 1971; Postman, 1963). Although it has been argued that overlearning may cost more resources through extended training beyond initial proficiency, this cost may be offset by lower costs associated with

subsequent retraining or refresher training. For example, Schendel and Hagman (1982) found that after an 8-week non-use interval, participants who received overlearning required 22% fewer trials to retrain to the criterion level than participants who did not receive overlearning.

Methodological Issues with Studies of Overlearning

Despite the vast number of studies supporting overlearning as an effective training strategy for bolstering retention, there are many methodological issues that challenge these findings and need to be addressed, some of which include how the criterion is defined and operationalized, the optimal retention interval, and the types of tasks examined. In many studies (e.g., Krueger, 1929; Postman, 1963; Schendel & Hagman, 1982), the criterion was operationally defined as achieving one errorless trial on a task, and the number of overlearning trials provided was determined by the number of trials it took participants to reach the criterion. For example, if it takes a participant 10 trials to reach one errorless trial on a task, 100% overlearning consisted of 10 additional trials. If it takes a different participant 20 trials to reach this criterion, 100% overlearning would consist of an additional 20 trials. Although this procedure ensures that all participants receive the precise level of initial learning (e.g., all participants actually reach the set criterion), these results are confounded by the overall amount of practice individuals receive (Rohrer et al., 2005). For example, participants who take longer to reach the criterion (e.g., 20 trials) may ultimately perform better on a retention task than those who reach the criterion much more quickly (e.g., 10 trials) simply due to the sheer amount of additional practice they are receiving.

To account for these issues, overlearning has also been manipulated through a duration-based approach where the duration of the study or the number of learning trials for each degree of learning is pre-determined. This approach ensures that all participants in the same learning condition receive an equal amount of learning trials or practice. However, it may difficult to establish an amount of practice that produces the desired degree of initial learning. Thus, with the duration-based approach, it is important for researchers to conduct pilot testing on a task to establish an appropriate amount of learning trials that should be provided. For example, Mandler (1954) conducted preliminary experiments to establish the smallest amount of training needed and set the criterion to 10 errorless trials based upon the extreme variability of task performance with training of less than 10 errorless trials. Similarly, Rohrer et al. (2005) pre-determined the number of learning trials in their study, which was set to five or 20 (referred to as low or high learning conditions, respectively). In addition, with a duration-based approach, it is possible for some participants to never reach an initial level of learning. Rohrer et al. (2005) stated that including these individuals in analyses may result in observed differences that overestimate the benefits of overlearning. Thus, they took into account this confound by conducting two separate sets of analyses, one comparing those in the low and high learning conditions and another further distinguishing these two learning groups by comparing those who had exceeded the criterion multiple times (referred to as the true high learners) and those who never reached the criterion (referred to as the true low learners).

In terms of retention intervals (i.e., the length of time after overlearning when trainees are tested again), Driskell et al. (1992) found that the benefits of overlearning

decreased by one half after 19 days and was found to disappear overall after a 5- to 6-week interval. Based on these findings, it was recommended that refresher trainings or courses be provided after approximately 3 weeks. However, out of the 15 studies included in Driskell et al.'s (1992) meta-analysis, only five studies included retention intervals greater than 1 week and only one greater than 28 days. In general, very few overlearning studies have examined retention intervals that exceed 1 month. Thus, the question left unanswered is whether overlearning is only beneficial for short-term retention. In this vein, Rohrer et al. (2005) examined retention intervals of 1, 3, and 9 weeks for a verbal recall task and found that although overlearning led to significantly greater recall, retention declined at a greater rate and by a greater proportion for those who underwent overlearning compared to those who did not receive overlearning. In other words, although overlearning is clearly advantageous after a short retention interval, the gains in retention may quickly diminish and both groups may ultimately be similar in terms of their recall or accuracy after an extended period of time has passed. Thus, further research is needed to determine whether the benefits of overlearning also apply to long-term retention.

In addition, with the exception of a few studies that have trained real-world or practical skills such as communication tactics or job-relevant skills (e.g., Kratzig, 2016; Lopez, 1980; Schendel & Hagman, 1982), the majority of overlearning studies have examined simple laboratory tasks such as verbal recall tasks. As stated by Driskell et al. (1992), "motivation certainly plays a role in training effectiveness…subjects will be more motivated to learn in studies that use relevant real-world tasks…than in studies that use laboratory tasks" (p. 621). Thus, participants in these studies may find no

relevance or importance to the tasks they are practicing, which may influence how well learning is retained. Further research should examine how overlearning influences retention with more complex tasks.

Hypotheses and Research Questions

The proposed study had two goals. The first goal of the study was to compare the effectiveness of rule-based and mindfulness training. To this aim, training effectiveness was measured in relation to skill retention on the performance of two different tests of phishing susceptibility: 1) an email identification test similar to their laboratory training task and 2) mock phishing attacks in their everyday (i.e., real-world) email use. Using these two tests was important due to the fact that they occur in different contexts. For example, identifying legitimate/phishing emails when one is provided with a predetermined set to solely focus on is very different from identifying legitimate/phishing emails when balancing other on-going demands. Thus, measuring retention through these two types of tests provided greater insight as to how well individuals learned to identify phishing emails versus their actual vulnerability to them in their everyday environment.

Consistent with previous studies that have compared anti-phishing training to a no training control condition (e.g., Kumaraguru et al., 2007b; Sheng et al., 2010), rule-based training should lead to better identification of phishing emails and less vulnerability to phishing attacks by providing individuals with a list of rules and cues commonly associated with phishing emails to work through when they are evaluating email messages. As mentioned previously, however, the effectiveness of rule-based training may be limited such that it constrains individuals from making decisions

outside of this predetermined list and turns the evaluation of emails into an automatic process. In this way, evaluating emails becomes more of a habit rather than a conscious task; thus, rule-based training still leaves individuals vulnerable to real phishing attacks (Vishwanath et al., 2011; Wright et al., 2014). On the other hand, mindfulness training can address these issues by promoting more systematic information processing when evaluating emails. By teaching individuals how to focus on the overall purpose and outcomes associated with emails and withhold quick judgments before allocating sufficient attention and time for evaluation, mindfulness training should be more effective than rule-based training in protecting individuals from phishing attacks (Baer, Smith, & Allen, 2004; Brown et al., 2007; Jensen et al., 2017). Regardless of the type of training (e.g., rule-based or mindfulness), however, receiving anti-phishing training should help individuals better identify phishing emails and be less vulnerable to falling for phishing attacks. Thus, the following two hypotheses were examined:

Hypothesis 1: Individuals who receive either rule-based training or mindfulness training will be a) better at identifying phishing emails and b) less vulnerable to phishing attacks in their everyday email use compared to individuals who do not receive anti-phishing training.

Hypothesis 2: Individuals who receive mindfulness training will be a) better at identifying phishing emails and b) less vulnerable to phishing attacks in their everyday email use compared to individuals who receive rule-based training.

In addition, very few studies have examined the retention of knowledge and skills taught during anti-phishing training, with all studies examining retention intervals that are less than 1 month (Alnajim & Munro, 2009; Kumaraguru et al., 2007;

Kumaraguru et al., 2009; Mayhorn & Nyeste, 2012). While the retention of knowledge and skills from anti-phishing training appear to be robust after these short retention intervals, further research is needed to examine how learning from anti-phishing training decays over longer retention intervals. Thus, the present study used a 2-month retention test interval.

In relation to the two anti-phishing training methods being compared, it is expected that individuals who receive mindfulness training should retain the knowledge and skills they gained during training for a longer period of time compared to individuals who receive rule-based training. Because mindfulness training teaches individuals to engage in the conscious evaluation of emails and elaborate on the cues they attend to, this greater depth of processing may result in better identification of phishing emails and less vulnerability to phishing attacks over an extended period of time (Craik & Lockhart, 1972; Petty & Cacioppo, 1986; Vishwanath et al., 2011). In contrast, learning from rule-based training is more superficial and may be more prone to decay as individuals only become familiar with the specific guidelines and cues they were provided during training. Although Jensen et al. (2017) only examined a 10-day retention interval, their findings support the effectiveness of mindfulness training versus rule-based training and warrant further investigation. Accordingly, the following hypothesis was examined:

> *Hypothesis 3*: Individuals who receive mindfulness training will have greater retention 2 months after training in terms of a) identifying phishing emails and b) being less vulnerable to phishing attacks in their everyday email use compared to individuals who receive rule-based training.

The second goal of the study was to examine the influence of overlearning on the two anti-phishing training methods in relation to retention. Because of the severe consequences associated with falling for phishing attacks, it is important to examine the impact of training strategies such as overlearning that can improve retention from anti-phishing training, which no studies have examined to my knowledge. Although overlearning should reinforce the knowledge and skills gained during training and help individuals better identify phishing emails and become less vulnerable to phishing attacks, overlearning in the context of anti-phishing training is unique in the sense that the task differs across situations. In other words, evaluating emails requires a level of generalizability because each email is composed differently. Because conscious effort needs to be applied when evaluating emails, overlearning may make individuals overly familiar with identifying phishing emails to the extent that they do not treat each email differently and thus process emails automatically. In this vein, overlearning may negatively impact retention after anti-phishing training over an extended period of time. Thus, the following research question was examined:

> *Research Question 1*: How does overlearning during training affect the a) identification of phishing emails and b) vulnerability to phishing attacks 2 months after training is completed?

In addition, rule-based and mindfulness training may affect skill retention differently as a function of overlearning. Overlearning in the context of rule-based training may help individuals grasp the rules and cues associated with phishing emails more quickly and lead to better identification of phishing emails and less vulnerability to phishing attacks. However, because rule-based training will likely lead to more

automatic email evaluation, overlearning may also exacerbate this effect by turning this task into a mindless habit more quickly. In this vein, overlearning may also be counterproductive to mindfulness training. Because overlearning is intended to increase automaticity in responses, this works against the purpose of mindfulness training, which is to help individuals allocate more attention and effort when evaluating emails. However, overlearning may also strengthen a more mindful approach by reinforcing System 2 thinking. Thus, the following research question was examined:

> *Research Question 2*: Are the effects of overlearning during training on a) the identification of phishing emails and b) vulnerability to phishing attacks in everyday email use different for rule-based and mindfulness training 2 months after training is completed?

Method

Participants

Students at the University of Oklahoma who were enrolled in an introductory management information systems course in the Price College of Business were recruited to participate in this study in exchange for course credit. A total of 517 students participated in the study. Of these 517 students, 47 students did not complete the second part of the study (i.e., the follow-up survey at Week 10), and an additional seven students provided incorrect email addresses which prevented them from receiving emails required throughout the study. Ten students were also flagged for having long strings of identical responses (i.e., bogus responding). These 64 students were thus removed from data analyses, yielding a final sample of 453 participants (55% male, 45% female). Participants ranged in age from 18 years to 42 years (M = 19.69, SD =

1.76). Three hundred and fifty (77.3%) participants reported their ethnicity as Caucasian, 30 (6.6%) as Asian, 21 (4.6%) as Native American, 19 (4.2%) as Hispanic/Latino, 15 (3.3%) as Black/African American, 4 (0.9%) as Multiple (i.e., two or more ethnicities), and 4 (0.9%) as Other. Ten (2.2%) participants did not disclose their ethnicity. Phishing also appeared to be relevant to this sample, as 192 (42.4%) participants knew of someone who has fallen for a phishing attack, and 28 (6.2%) participants indicated that they have personally fallen for a phishing attack themselves.

General Procedures

Figure 1 displays the general study procedures. Participants first attended an in-person training session administered on the computer through the online survey platform Qualtrics. After agreeing to participate in the study, participants were introduced to the 1-hour training session and told that the purpose of this study was to test a new cybersecurity training and help individuals distinguish legitimate from phishing emails. Participants first completed a series of Likert-scale measures of the covariates related to their email, web, and past phishing experiences, as well as personality traits related to these experiences. Participants then received one of three trainings (rule-based, mindfulness, or control [i.e., password creation and management] training). Afterwards, participants received one of two email identification practice sessions (i.e., no overlearning or 100% overlearning) where they read a series of email messages and identified whether or not each message is a phishing message. Practice sessions differed in terms of how many email messages participants received during practice (i.e., six emails for the no overlearning condition and 12 emails for the 100%

overlearning condition). The number of practice emails used for each condition was determined through pilot testing and previous research (e.g., Jensen et al., 2017).

After completing the practice session and a filler task (i.e., Big Five personality measure), participants completed the first email identification test. Participants then completed basic demographic questions and were debriefed about the training they received. Finally, participants were reminded that they would be tested throughout the semester with mock phishing attacks and would be invited to take a follow-up online survey towards the end of the semester to receive additional course credit for their participation.

One week after completing the training session, participants received the first test of vulnerability to mock phishing attacks (i.e., first round of mock phishing attacks). Eight weeks later, the second test of vulnerability to mock phishing attacks (i.e., second round of mock phishing attacks) occurred. After the second test of vulnerability to mock phishing attacks occurred, participants were emailed the follow-up online survey consisting of a second email identification test, reinforcement of training to provide anti-phishing training to those in the control training group, and a full debrief of the study.

Training Conditions

Participants were randomly assigned to one of three training conditions: rule-based training, mindfulness training, or a control training condition. Training content was constructed on Qualtrics and delivered through a series of webpages that included text and graphics. Participants worked through the webpages individually, and all content for the three training conditions were adapted from materials previously

developed by Jensen et al. (2017). Before receiving information specific to their training conditions, participants in the rule-based and mindfulness training conditions first received the same introductory content that provided background information on what phishing is, the current state and recent statistics of phishing attacks, and the consequences of being a victim of phishing (see Appendix A). The purpose of this introduction was to highlight the importance of the training and motivate participants to take the training seriously by making their perceived risk of phishing more salient. Participants in the control condition did not receive any information related to phishing and were instead provided with training materials regarding how to create and manage more secure passwords (see Appendix B).

The rule-based training content consisted of a list of recommendations derived from guidelines from various anti-phishing resources in the academic, governmental, non-profit, and corporate sectors. This list was previously presented to information technology (IT) security managers at the university to ensure that the material is relevant and useful for reducing phishing susceptibility. The list consisted of six recommendations that were used as the content for the rule-based training (see Appendix C).

The mindfulness training content consisted of materials that were based on previous clinical research on mindfulness and adapted to an anti-phishing context. This training approach focused on three key steps: 1) stop, 2) think, and 3) check. In the first step, individuals were advised to pause before taking any actions requested in an email (e.g., clicking a link, replying to the email, or downloading an attachment). By not taking immediate action, individuals can remind themselves of the potential

consequences and outcomes of abiding by the email's request. In the second step, individuals were advised to consider four questions (see Appendix D) which asked them to reflect upon the actions being requested, the overall context in which the requests were received, and the underlying motive behind the sender's request. Finally, in the third step, individuals were encouraged to check with a third-party source (e.g., university IT help desk) if they were unsure about the legitimacy of the email. Participants who received either rule-based or mindfulness training were also shown examples of legitimate and phishing emails, as well as explanations consistent with the type of training they received (see Appendix E).

Overlearning Conditions

For the email identification practice session, participants were assigned to one of two overlearning conditions: no overlearning or 100% overlearning. Although the optimal amount of overlearning required is different depending on the type of task, there is support suggesting that a minimum of 50% overlearning is beneficial and that increases from 100% to 150% do not result in greater retention (Craig, Sternthal, & Olshan, 1972; Krueger, 1929; Schendel & Hagman, 1982). Thus, the present study used 100% overlearning.

During the email identification practice session, participants in both conditions were first provided with the same six emails (three legitimate and three phishing emails; see Appendix F). These six emails were displayed in a randomized order. Once participants in the no overlearning condition worked through these six email messages, they were finished with the email identification practice session. However, participants in the 100% overlearning condition were provided with additional practice through an

additional six emails to identify (three legitimate and three phishing emails; see Appendix G). These additional six emails were also displayed in a randomized order. Feedback regarding correct/incorrect answers was provided after each email message during the email identification practice session, and explanations for correct answers were consistent with the type of training participants received, with the exception of those in control condition who did not receive explanations. Feedback provided during the email identification practice session is similar to the feedback shown in the example legitimate and phishing emails in Appendix E.

Based on previous performance on an email identification task from Jensen et al. (2017), the learning criterion was set to correctly identifying four of the six practice emails. Following similar procedures utilized by previous researchers (e.g., Rohrer et al., 2005; Rohrer & Taylor, 2006), if participants did not correctly identify four email messages, it was assumed that they did not reach a meaningful level of learning. Because of this potential confound, supplemental analyses were conducted to compare results of the overall sample with a sample excluding participants who did not reach the required level of learning.

Learning Measures

Emails included in the present study were developed and also derived from previous studies (e.g., Jensen et al., 2017). Pilot testing was conducted with 86 students enrolled in psychology and management information systems courses to ensure equal difficulty across all emails included throughout the study (e.g., the two versions of the email identification tests and two versions of the tests of vulnerability to mock phishing attacks). Based on recommendations by Myers (2007), emails were designed to be

applicable and relevant to current university students and were based on actual legitimate and phishing emails. For the email identification tests, all links embedded in the emails consisted of URLs that redirected participants who clicked on them to either legitimate websites associated with the source being portrayed or purchased web domains that then redirected participants to legitimate websites associated with the source being portrayed. For example, a legitimate email from Netflix included a link to the actual Netflix website (e.g., https://www.netflix.com), whereas a phishing email from Netflix included a link to a web domain that resembled the actual Netflix website (nef1ix.com) and redirected participants to the legitimate Netflix website. For the tests of vulnerability to mock phishing attacks, all links embedded in the emails were generated by the Wombat Security Education Platform used to distribute the mock phishing emails. Although the Wombat Security Education Platform provides "teachable moments" and informs individuals that they have fallen for a phishing attack if they click on the links, these links were instead designed to redirect participants who clicked on them to an error page to reduce suspicion of other mock phishing emails being distributed during that timeframe.

Email identification tests

Participants completed the first email identification test after completing the practice session during the in-person training session. This test was similar to the email identification practice session but did not include feedback. The test consisted of 10 email messages (five phishing and five legitimate) that appeared in a randomized order. After 10 weeks (at the conclusion of the second test of vulnerability to mock phishing attacks [i.e., second round of mock phishing attacks]), participants received the second

email identification test, which also included 10 email messages, that was emailed to participants through an online survey. These 10 emails were different from those included in the first email identification test. The two versions of the email identification tests were counterbalanced. In terms of scoring for the email identification tests, scores were calculated based on the total number of emails that participants correctly identified. Appendices H and I display the emails included in Versions 1 and 2 of the email identification tests, respectively. The percentage of correct responses in the pilot sample was 68% for both Versions 1 and 2 of the email identification tests.

Mock phishing attacks

One week after the training session, participants received the first test of vulnerability to mock phishing attacks. This test included five mock phishing emails sent to participants, which was distributed throughout a 2-week interval to reduce suspicion from receiving too many phishing messages within a short time period. Eight weeks after the training session, participants received the second test of vulnerability to mock phishing attacks, which also included five mock phishing emails. These five mock phishing emails were different from the five mock phishing emails included in the first test and were also distributed throughout a 2-week interval. The two versions of the tests of vulnerability to mock phishing attacks were counterbalanced. Additionally, the order of the five mock phishing emails within each test, as well as the dates and times they were distributed during the 2-week intervals, were randomized to minimize the likelihood of participant interactions related to these emails. In terms of scoring for the tests of vulnerability to mock phishing attacks, scores were calculated based on whether individuals clicked on the links embedded in the mock phishing emails and then

reversed such that higher scores reflected better performance (i.e., less vulnerability). All clicks made on the email links were tracked through the Wombat Security Education Platform. Appendices J and K display the emails included in Versions 1 and 2 of the tests of vulnerability to mock phishing attacks, respectively. The percentage of correct responses in the pilot sample was 67% and 68% for Versions 1 and 2 of tests of vulnerability to mock phishing attacks, respectively. It is important to note that the tests of vulnerability to mock phishing attacks were not pilot tested through mock phishing attacks; rather, these tests were piloted similarly to the email identification tests by having the pilot sample indicate whether or not each message was a phishing message.

Kumaraguru et al. (2009) outlined a series of issues that should be addressed when designing studies that utilize mock phishing attacks in real-world settings, which include ensuring that emails sent to participants actually reach their inboxes, maintaining participants' privacy, and coordinating with relevant third parties associated with the study. To address these issues, a list of mock phishing emails that were used in the study was provided to the university's information technology (IT) department prior to the beginning of the study to ensure that the emails were not blocked from the university's server. In the event that participants contacted the IT department regarding the mock phishing emails they received, actions were not taken on any participant inquiries or concerns to minimize information regarding the nature of the emails from being revealed. When participants received the mock phishing emails, they could have responded in one of three ways: 1) opened the email and clicked on the embedded link; 2) opened the email but did not click on the embedded link; or 3) did not open the email and did not click on the embedded link. Although some participants

did not open the emails they received, it is assumed that participants still received and saw these emails regardless because these emails were sent to participants' university-affiliated email addresses from which they accessed the online survey link containing the second email identification test that had to be completed to be included in data analyses. In this vein, participants may have still read the emails without actually opening them by viewing them in the preview pane within their email clients.

In addition, because email reading behavior may differ at various periods of time (e.g., weekends, late hours), mock phishing emails were not scheduled during these times and were only sent during typical work hours (i.e., Monday to Friday, 9:00am to 5:00pm). In addition, the proposed study received approval from the university's Institutional Review Board (IRB) and thus followed all procedures necessary to ensure participants' privacy throughout the course of the study. Participants were informed prior to the beginning of the study that they would be sent mock phishing emails throughout the course of the semester to evaluate the effectiveness of the training they would receive. Additionally, participants were fully debriefed about the study at the conclusion of the study (i.e., after completing the second email identification test in the online survey). Oral presentations were also given to participants' classes to provide study results and reinforce the training participants received.

Covariates

Based on previous research by Wright and Marett (2010), the following variables were included as covariates due to their relationship to phishing susceptibility and training efficacy.

Disposition to trust

Disposition to trust was measured using four items adapted from McKnight, Choudhury, and Kacmar's (2002) scale. Participants were asked to respond on a 7-point Likert scale (1 = *strongly disagree* to 7 = *strongly agree*). An example item was "I usually trust people unless they give me a reason not to trust them." The coefficient alpha obtained for this scale was .87.

Mindfulness in technology

Mindfulness in technology was measured using four items from Thatcher, Wright, Sun, Klein, and Zagenczyk's (2017) scale. Participants were asked to respond on a 7-point Likert scale (1 = *strongly disagree* to 7 = *strongly agree*). An example item was "I am often open to learning new ways of using technology." The coefficient alpha obtained for this scale was .89.

Perceived Internet risk

Perceived Internet risk was measured using five items adapted from Malhotra, Kim, and Agarwal's (2004) scale. Participants were asked to respond on a 7-point Likert scale (1 = *strongly disagree* to 7 = *strongly agree*). An example item was "In general, it would be risky to give my information to online companies." The coefficient alpha obtained for this scale was .87.

Computer self-efficacy

Computer self-efficacy was measured with six items adapted from Compeau and Higgin's (1995) scale. This scale included three items each for internal computer self-efficacy and external computer self-efficacy. Participants was asked to respond on a 10-point Likert scale (1 = *not at all confident* to 10 = *totally confident*). Example items for

internal computer self-efficacy and external computer self-efficacy were "I could complete my job using a new software application if there was no one around to tell me what to do as I go" and "I could complete the job using a new software application if someone showed me how to do it first", respectively. The coefficient alphas obtained for internal and external computer self-efficacy were .86 and .84, respectively.

Phishing identification expertise

Phishing experience was measured using three items from Jensen et al. (2017). Participants were asked to respond on a 7-point Likert scale (1 = *strongly disagree* to 7 = *strongly agree*). An example item was "I know what a phishing message looks like." The coefficient alpha obtained for this scale was .85.

Email experience

Email experience was measured using three items from Jensen et al. (2017). Participants were asked to respond on a 7-point Likert scale (1 = *strongly disagree* to 7 = *strongly agree*). An example item was "I can process new emails in my inbox rapidly." The coefficient alpha obtained for this scale was .88.

Pre-training motivation

Pre-training motivation was measured using three items adapted from Noe and Schmitt's (1986) scale. Participants responded on a 5-point Likert scale (1 = *strongly disagree* to 7 = *strongly agree*). An example item was "I am motivated to learn the skills emphasized in this training program." The coefficient alpha obtained for this scale was .87.

Big Five personality

Extraversion, conscientiousness, openness to experience, emotional stability, and agreeableness were measured using Goldberg's (1981) 100-item scale. This scale included 20 items for each of the five personality constructs. Participants were asked how accurately each trait describes them and were asked to respond on a 9-point Likert scale (1 = *extremely inaccurate* to 9 = *extremely accurate*). Example items for extraversion, conscientiousness, openness to experience, emotional stability, and agreeableness were "active", "careful", "deep", "relaxed", and "cooperative", respectively. The coefficient alphas obtained for these extraversion, conscientiousness, openness to experience, emotional stability, and agreeableness were .89, .88, .77, .84, and .81, respectively.

Results

Table 1 provides a summary of the results found for the study hypotheses and research questions. Table 2 displays the means, standard deviations, reliabilities, and correlations for the study variables. Two 3 (training method: rule-based, mindfulness, or control training) × 2 (overlearning: 100% overlearning or no overlearning) × 2 (test administration: Time 1 and Time 2) mixed-design analyses of covariance (ANCOVAs) were conducted — one for the email identification tests and the other for the tests of vulnerability to mock phishing attacks. Tables 3 and 4 display the adjusted means and standard errors for the email identification tests and tests of vulnerability to mock phishing attacks, respectively. Although all covariates were included in the initial analyses, the majority of covariates did not yield statistically significant effects.

Additional models that excluded nonsignificant covariates were run and did not yield results that would warrant different conclusions. Thus, reported results only included tests that included statistically significant covariates.

Main Effects of Training

To test Hypotheses 1 and 2, the main effects of training for the scores on the email identification tests and tests of vulnerability to mock phishing attacks were examined, which included two planned comparisons. As shown in Table 5, there was a significant main effect of training for the email identification tests, $F(1, 446) = 19.92$, $p < .001$, $\eta_p^2 = .08$. As seen in Figure 2, planned comparisons revealed that individuals who received anti-phishing training (i.e., either rule-based training or mindfulness training; $M = 7.36$, $SE = .07$) had significantly higher mean scores on the email identification tests compared to those who did not receive anti-phishing training (i.e., control training; $M = 6.84$, $SE = .10$, $p < .001$). Thus, Hypothesis 1a was supported. Additionally, individuals who received mindfulness training ($M = 7.71$, $SE = .10$) had significantly higher mean scores on the email identification tests compared to those who received rule-based training ($M = 7.04$, $SE = .10$, $p < .001$). Thus, Hypothesis 2a was supported.

As shown in Table 6 and Figure 3, there was a significant main effect of training for the tests of vulnerability to mock phishing attacks, $F(1, 447) = 5.17$, $p < .01$, $\eta_p^2 = .02$. Planned comparisons revealed that individuals who received anti-phishing training (i.e., either rule-based training or mindfulness training; $M = 4.38$, $SE = .04$) did not significantly differ in their mean scores on the tests of vulnerability to mock phishing attacks compared to those who did not receive anti-phishing training (i.e., control

training; $M = 4.26$, $SE = .06$, $p = .12$). Thus, Hypothesis 1b was not supported. Although individuals who received rule-based training ($M = 4.26$, $SE = .06$) versus the control training ($M = 4.26$, $SE = .06$) did not differ in their mean scores on the tests of vulnerability to mock phishing attacks, individuals who received mindfulness training ($M = 4.49$, $SE = .06$) had significantly higher mean scores on the tests of vulnerability to mock phishing attacks (i.e., were less vulnerable to mock phishing attacks) compared to those who received the rule-based or control training ($ps < .05$). Thus, Hypothesis 2b was supported.

Effects of Training on Retention

Hypothesis 3 was tested in two ways. First, I examined the training method and test administration interaction to examine retention/decay (i.e., changes in scores between Time 1 and Time 2). Second, I examined test scores at Time 2 with planned comparisons focused on differences between the rule-based and mindfulness training conditions to compare the sheer levels of performance 2 months after training.

As seen in Table 5, there was a significant interaction between training and test administration for scores on the email identification tests, $F(1, 446) = 4.60$, $p < .05$, $\eta_p^2 = .02$. As seen in Figure 2, individuals who received rule-based or mindfulness training had significantly lower scores (i.e., decay) on the email identification test at Time 2 compared to Time 1 (mean difference of -.60 and -.45 for rule-based and mindfulness trainings, respectively; $ps < .01$), whereas individuals who received the control training did not have significantly different scores between Time 1 and Time 2 (mean difference of .06; $p = .70$; the scores remained at low levels). Although there was a significant change in scores on the email identification tests between Time 1 and Time 2 for

individuals who received rule-based and mindfulness training, the change in scores on the email identification tests was not different between those that received the two types of training.

In terms of test scores on the email identification test at Time 2, planned comparisons revealed that individuals who received mindfulness training (M = 7.48, SE = .13) scored significantly higher on the email identification test at Time 2 compared to those who received rule-based (M = 6.74, SE = .13, $p < .001$) or the control training (M = 6.87, SE = .13, $p < .01$, respectively). There was no difference in scores for the email identification test at Time 2 between individuals who received rule-based or the control training, p = 1.00. Overall, Hypothesis 3a was supported in terms of the sheer level of performance on the email identification test 2 months after training between individuals that received rule-based versus mindfulness training but not supported in terms of the amount of retention/decay across the 2 months.

As shown in Table 6, there was not a significant interaction between training and test administration for the scores on the tests of vulnerability to mock phishing attacks, $F(1, 446) = .75$, $p = .47$, $\eta_p^2 = .00$. In other words, as seen in Figure 3, the changes in scores on the tests of vulnerability to mock phishing attacks between Time 1 and Time 2 were not significantly different between those who received rule-based (mean difference of -.12) versus mindfulness training (mean difference of -.08). In terms of scores on the test of vulnerability to mock phishing attacks at Time 2, planned comparisons revealed that individuals who received mindfulness training (M = 4.53, SE = .07) did not score significantly higher on the test of vulnerability to mock phishing attacks at Time 2 compared to those who received rule-based (M = 4.32, SE = .07, p =

.07) or the control training (M = 4.38, SE = .07, p = .35, respectively). Additionally, there was no difference in scores for the test of vulnerability to mock phishing attacks at Time 2 between individuals who received rule-based or the control training, p = 1.00. Overall, Hypothesis 3b was not supported for the sheer level of performance on the test of vulnerability to mock phishing attacks 2 months after training or the degree of retention/decay on the test of vulnerability to mock phishing attacks across the 2 months between individuals that received rule-based versus mindfulness training. Although the results for scores at Time 2 did not reach conventional levels of statistical significance (p = .09), they were in the predicted direction such that individuals who received mindfulness training had higher scores on the test of vulnerability to mock phishing attacks at Time 2 than individuals who received either rule-based or the control training.

Effect of Overlearning on Retention

Research Question 1 was tested in two ways. First, I examined the overlearning and test administration interaction to examine retention/decay (i.e., changes in scores between Time 1 and Time 2). Second, I examined test scores at Time 2 to compare the sheer levels of performance 2 months after training between the 100% overlearning and no overlearning conditions.

As shown in Table 5, there was not a statistically significant interaction between overlearning and test administration on retention for the email identification tests, F(1, 446) = 1.59, p = .21, η_p^2 = .00. In other words, the changes in scores on the email identification tests between Time 1 and Time 2 were not significantly different between individuals who received 100% overlearning (mean difference of -.46) versus no overlearning (mean difference of -.20). Similarly, there was not a significant difference

in scores on the email identification test at Time 2 between individuals who received 100% overlearning ($M = 7.04$, $SE = .10$) versus no overlearning ($M = 7.02$, $SE = .11$, $p = .92$).

As shown in Table 6, there was not a statistically significant interaction between overlearning and test administration for the scores on the tests of vulnerability to mock phishing attacks, $F(1, 447) = .74$, $p = .11$, $\eta_p^2 = .00$. In other words, the changes in scores on the tests of vulnerability to mock phishing attacks between Time 1 and Time 2 were not significantly different between individuals who received 100% overlearning (mean difference of .16) versus no overlearning (mean difference of .13). Similarly, there was not a significant difference in scores on test of vulnerability to mock phishing attacks at Time 2 between individuals who received 100% overlearning ($M = 4.47$, $SE = .05$) versus no overlearning ($M = 4.35$, $SE = .06$, $p = .13$).

Although the results showed that receiving 100% overlearning did not result in significantly better retention compared to receiving no overlearning, there was a significant main effect of overlearning for scores on the tests of vulnerability to mock phishing attacks, $F(1, 447) = 4.11$, $p < .05$, $\eta_p^2 = .01$. In other words, as seen in Figure 4, individuals who received 100% overlearning ($M = 4.41$, $SE = .05$) had significantly higher mean scores on both tests of vulnerability to mock phishing attacks on average (i.e., were less vulnerable to mock phishing attacks) compared to those who did not receive overlearning ($M = 4.27$, $SE = .05$). Thus, receiving additional practice may still be beneficial in terms of helping individuals become less vulnerable to mock phishing emails overall.

Effect of Training Method and Overlearning on Retention

Research Question 2 was tested in two ways. First, I examined the training method, overlearning, and test administration interaction to examine retention/decay (i.e., changes in scores between Time 1 and Time 2). Second, I examined the training method and overlearning interaction at Time 2 to compare sheer levels of performance 2 months after training.

As shown in Tables 5 and 6, there were no statistically significant interactions between training, overlearning, and test administration for the email identification tests, $F(1, 446) = 2.33$, $p = .10$, $\eta_p^2 = .01$, or the tests of vulnerability to mock phishing attacks, $F(1, 447) = 1.28$, $p = .28$, $\eta_p^2 = .01$. In other words, the change in scores on the email identification tests and tests of vulnerability to mock phishing attacks from Time 1 to Time 2 were not significantly different between the combinations of training (i.e., rule-based or mindfulness) and overlearning (i.e., 100% overlearning and no overlearning). Similarly, as shown in Table 8, there were no statistically significant interactions between training and overlearning on scores for the email identification tests, $F(1, 446) = .53$, $p = .59$, $\eta_p^2 = .00$, or the tests of vulnerability to mock phishing attacks, $F(1, 447) = 1.43$, $p = .24$, $\eta_p^2 = .01$, at Time 2. Thus, the results showed that the effects of training and overlearning are not dependent upon one another. Put another way, the beneficial effects of mindfulness training do not differ as a function of overlearning.

Supplemental Analyses

Signal Detection Theory

In addition to examining the overall scores of the email identification tests, I also conducted supplemental analyses to gain insight regarding how training and overlearning affected individuals' capability to detect phishing messages and their caution towards phishing by applying Signal Detection Theory (SDT) methods (Green & Swets, 1966; Macmillan & Creelman, 2004; Swets, Dawes, & Monahan, 2000). SDT is often used in research contexts such as medical decision making and memory recognition, and previous researchers have also extended SDT methods to phishing detection (Canfield, Fischhoff, & Davis, 2016; Kumaraguru et al., 2010; Sheng et al., 2007). In general, SDT quantifies the capability to distinguish between signals (stimuli) and noise (no stimuli). Within a phishing detection context, signals refer to phishing websites, whereas noise refers to legitimate websites. As seen in Figure 5, there are four types of responses possible in a phishing detection task: 1) hits (i.e., correctly identifying a phishing email as phishing); 2) misses or false negatives (i.e., incorrectly identifying a phishing email as legitimate); 3) correct rejections (i.e., correctly identifying a legitimate email as legitimate); and 4) false positives (incorrectly identifying a legitimate email as phishing). Applying SDT methods is valuable beyond examining solely accuracy rates because it accounts for the trade-offs made between hit rates and false positive rates.

Based on these responses, SDT provides a means of estimating two different indices: 1) discriminability/sensitivity (*d'*) and 2) response bias/criterion (*c*). *d'* refers to an individual's capability to tell whether an email is phishing or legitimate such that the larger the value of *d*', the greater the distance between the means of the signal and noise

distributions (see Figure 6; Sheng et al., 2007). In other words, larger values of *d'* indicate that users have greater discriminability/sensitivity and are able to better distinguish between legitimate and phishing emails. On the other hand, *c* refers to an individual's tendency or willingness to treat an email as phishing. It is important to note that *c* is separate from *d'* such that two users may have the same value of *d'* (i.e., they have the same capability in discriminating between legitimate and phishing emails) but may be more or less biased in their responses or the criterion they set for labeling an email as phishing. For example, some individuals may be more cautious in their responses and thus more likely to label all emails as phishing (i.e., higher hit rates and false positives), whereas more vulnerable individuals only label a small number of emails as phishing. Negative values of *c* indicate that users are erring on the side of caution (i.e., more likely to label an email as being phishing), whereas positive values of *c* indicate that users are especially vulnerable to phishing (i.e., less likely to label an email as being phishing). Overly cautious users are more likely to have higher hit rates but also higher false positive rates. On the other hand, other users are more likely to have lower false positive rates but also lower hit rates. Ideally, anti-phishing training should make users more cautious of phishing in their email evaluations (i.e., result in lower, negative values of *c*), but it should also help users distinguish between legitimate and phishing emails (i.e., result in higher values of *d'*).

For these supplemental analyses, *d'* and *c* were first calculated using estimates of hit rates and false positive rates (see Macmillan and Creelman [1990] for *d'* and *c* index calculation formulas). Next, two 3 (training method: rule-based, mindfulness, or control training) × 2 (overlearning: 100% overlearning or no overlearning) × 2 (test

administration: Time 1 and Time 2) mixed-design ANCOVAs were conducted for *d'* and *c* as two additional dependent variables. Tables 7 and 8 display the adjusted means and standard errors for *d'* and *c* for the email identification tests at Time 1 and Time 2, respectively.

Effect of training and overlearning on d'

In general, the effects of training and overlearning on *d'* are similar to the effects of training and overlearning on scores on the email identification tests. As seen in Table 9, there was a significant main effect of training on *d*', $F(1, 446) = 18.45$, $p < .001$, $\eta_p^2 = .08$. The results showed that individuals who received mindfulness training ($M = 1.38$; $SE = .06$) had significantly greater discriminability between phishing and legitimate emails compared to those who received rule-based ($M = 1.05$; $SE = .05$) or the control training ($M = .92$; $SE = .05$; $ps < .001$). However, individuals who received rule-based training did not have significantly different discriminability between phishing and legitimate emails compared those who received the control training ($p = .32$).

Additionally, there was a significant interaction between training and test administration on *d*', $F(1, 446) = 5.41$, $p < .01$, $\eta_p^2 = .02$. As seen in Figure 7, individuals who received rule-based or mindfulness training had significantly less discriminability between legitimate and phishing emails at Time 2 compared to Time 1 (mean difference of -.34 and -.24 for rule-based and mindfulness trainings, respectively; $ps < .01$), whereas individuals who received the control training did not have significantly different discriminability between phishing and legitimate emails between Time 1 and Time 2 (mean difference of .05; $p = .58$). Although there was a significant change in *d'* on the email identification tests between Time 1 and Time 2 for individuals

who received rule-based or mindfulness training, the change in *d'* on the email identification tests was not different between those that received rule-based versus mindfulness training.

In terms of *d'* at Time 2, planned comparisons revealed that individuals who received mindfulness training ($M = 1.25$, $SE = .07$) had significantly greater discriminability between phishing and legitimate emails at Time 2 compared to those who received rule-based ($M = 8.76$, $SE = .07$, $p < .001$) or the control training ($M = .95$, $SE = .07$, $p < .01$, respectively). Individuals who received rule-based training, however, did not differ in their discriminability between phishing and legitimate emails at Time compared to those who received the control training, $p = 1.00$.

Additionally, there was not a significant main effect of overlearning on *d*', $F(1, 446) = 1.30$, $p = .25$, $\eta_p^2 = .00$. In other words, individuals who received 100% overlearning ($M = 1.15$; $SE = .04$) did not differ in their discriminability between phishing and legitimate emails compared to those who did not receive overlearning ($M = 1.08$; $SE = .04$). There was also not a significant interaction between overlearning and test administration on *d*', $F(1, 446) = 1.53$, $p = .22$, $\eta_p^2 = .00$. In other words, the changes in discriminability between phishing and legitimate emails between Time 1 and Time 2 were not significantly different between individuals who received 100% overlearning (mean difference of -.24) versus no overlearning (mean difference of -.11). Similarly, there was not a significant difference in discriminability between phishing and legitimate emails at Time 2 between individuals who received 100% overlearning ($M = 1.03$, $SE = .05$) versus no overlearning ($M = 1.02$, $SE = .06$, $p = .92$). There was also not a significant interaction between training, overlearning, and test administration

on *d'*, $F(1, 446) = 2.26$, $p = .11$, $\eta_p^2 = .01$. In other words, the change in *d'* from Time 1 to Time 2 was not significantly different between the combinations of training (i.e., rule-based or mindfulness) and overlearning (i.e., 100% overlearning and no overlearning).

Effect of training and overlearning on c

As seen in Table 10, there was a significant main effect of test administration on *c*, $F(1, 447) = 47.20$, $p = < .001$, $\eta_p^2 = .10$. The results showed that individuals became significantly more cautious of phishing in their responses at Time 2 compared to Time 1 (mean difference of -.18; $p < .001$). Additionally, there was a significant interaction between training and test administration on *c*, $F(1, 447) = 6.70$, $p = < .01$, $\eta_p^2 = .03$. As seen in Figure 8, individuals who received rule-based or the control training were significantly more cautious of phishing in their responses at Time 2 compared to Time 1 (mean difference of -.18 and -.28 for rule-based and the control trainings, respectively; *p*s < .001), whereas individuals who received the mindfulness training did not significantly differ in their response bias between Time 1 and Time 2 (mean difference of -.05; $p = .22$). In fact, at Time 2, individuals who received mindfulness training ($M = -.10$, $SE = .04$) did not differ in their response bias compared to those who received rule-based training ($M = -.09$, $SE = .03$, $p = 1.00$) or the control training ($M = -.18$, $SE = .04$, $p = .36$) Although there was no change in response bias between Time 1 and Time 2 for those who received mindfulness training, individuals who received mindfulness training were significantly more cautious of phishing in their responses at Time 1 compared to those who received the rule-based (mean difference of -.14) or the control training (mean difference of -.15; *p*s < .01). Thus, the results showed that individuals

who received mindfulness training maintained their level of caution towards phishing throughout the 10-week period.

Additionally, as seen in Figure 9, there was a significant main effect of overlearning on *c*, $F(1, 447) = 4.62$, $p = < .05$, $\eta_p^2 = .01$. The results showed that individuals who received 100% overlearning ($M = -.07$, $SE = .02$) were significantly more cautious of phishing in their responses compared to those who did not receive overlearning ($M = -.01$, $SE = .02$). However, there was not a significant interaction between overlearning and test administration on *c*, $F(1, 446) = 1.53$, $p = .22$, $\eta_p^2 = .00$. In other words, the changes in caution towards phishing between Time 1 and Time 2 were not significantly different between individuals who received 100% overlearning(mean difference of -.21) versus no overlearning (mean difference of -.14). There was also not a significant difference in response bias at Time 2 between individuals who received 100% overlearning ($M = -.14$, $SE = .03$) versus no overlearning ($M = -.11$, $SE = .03$, $p = .42$). Even so, individuals who received 100% overlearning ($M = .00$, $SE = .03$) were significantly more cautious of phishing at Time 1 compared to those who did not receive overlearning ($M = .10$, $SE = .03$, $p < .05$). There was also not a statistically significant interaction between training, overlearning, and test administration *c*, $F(1, 447) = 0.89$, $p = .41$, $\eta_p^2 = .00$. In other words, the change in *c* from Time 1 to Time 2 was not significantly different between the combinations of training (i.e., rule-based or mindfulness) and overlearning (i.e., 100% overlearning and no overlearning).

Inclusion of "True" Learners

As mentioned previously, additional analyses were conducted to compare the results of the overall sample ($N = 453$) with the results of the "true" learner sample ($N = 300$) that only included those who reached the criterion level of learning of at least four correctly identified emails on the practice test. With the exception of non-significant main effects of overlearning on the tests of vulnerability to mock phishing attacks and on *c* for the email identification tests (*p*s > .05), the pattern of effects for the "true" learner sample on the remaining tests were of the same or similar magnitudes and reached the same or similar levels of significance compared to the overall sample.

Discussion

The present study extends the work of Jensen et al. (2017) by comparing the effectiveness of rule-based and mindfulness training for a longer retention interval (i.e., 10 days versus 2 months) and on two tests of skill retention of phishing susceptibility (i.e., email identification and mock phishing attack tests). Additionally, this study examined overlearning as a potential training strategy to improve skill retention on these two tests. The results showed that mindfulness training was significantly more beneficial compared to rule-based training in terms of helping individuals discriminate between legitimate and phishing emails (*d'*), become more cautious of phishing (*c*), and become less susceptible to falling for phishing attacks overall. Although the discriminability effect of mindfulness training was shown to decay similar in rate to rule-based training, the overall effects of mindfulness training were far superior compared to those of rule-based training. Overlearning, however, did not improve skill retention or help individuals better discriminate between legitimate and phishing emails.

It was, however, beneficial in terms of increasing individuals' caution towards phishing and making individuals less susceptible to phishing attacks. In the following sections, I review the findings on anti-phishing training (i.e., rule-based and mindfulness training) and overlearning on my two tests of skill retention of phishing susceptibility, as well as the practical implications of my study. Finally, I discuss limitations of my study and avenues for future researchers to consider.

Anti-Phishing Training on Phishing Identification and Susceptibility

Previous research has shown that anti-phishing training can be an effective strategy for helping individuals learn how to identify phishing emails and become less susceptible to phishing attacks (Karumbaiah et al. 2016; Kumaraguru et al., 2007b; Sheng et al., 2007; Sheng et al., 2010). However, the majority of these studies have relied primarily upon training that follows a rule-based approach that teaches individuals how to apply certain rules or attend to various cues associated with phishing when they evaluate emails. As phishers become increasingly sophisticated with their attack methods that extend beyond these common rules and cues, it is necessary for anti-phishing training to also evolve and incorporate content that can help individuals apply strategies more broadly when evaluating emails. In this vein, Jensen et al. (2017) designed an anti-phishing training program that incorporated mindfulness techniques to help individuals better allocate their attention during message evaluation, actively question requests made within messages, and forestall action concerning suspicious messages. By having individuals think more broadly about the contexts in which they receive email messages, mindfulness training can overcome the limitations of rule-based training.

The results of the present study support the initial findings of Jensen et al. (2017) by showing beneficial effects of mindfulness training. Specifically, compared to those who received rule-based training and the control training, individuals who received mindfulness training had significantly higher scores on the email identification tests. SDT analyses further elaborate on these results by showing that individuals who received mindfulness training were much better at discriminating between legitimate and phishing messages compared to those who received rule-based training or the control training. The results also show how the benefits of mindfulness training extend beyond the lab setting to the field. In other words, individuals who received mindfulness training were able to transfer the knowledge and skills they gained from training to their everyday email usage, indicated by significantly lower click rates on the mock phishing email links compared to those who received rule-based training or the control training. Even so, as seen in Figures 2 and 7, the effects of mindfulness training in terms of the identification test still appear to decay over time, indicated by significantly lower scores at Time 2 compared to Time 1. This decay indicates the need for individuals to take refresher courses to retain the knowledge and skills gained from mindfulness training. Although this rate of decay is similar to that of rule-based training, the change in scores does not undermine the finding that mindfulness training is still an effective training method and results in better email discriminability and less susceptibility to phishing attacks compared to rule-based training and the control training. These findings also indicate that mindfulness training can reduce susceptibility to phishing attacks and not at the expense of higher false positive rates (i.e., missing legitimate emails by incorrectly labeling them as phishing). In other words, because

mindfulness training also resulted in better discriminability, individuals who received mindfulness training can protect themselves from phishing attacks without disrupting their work productivity by being able to recognize and respond to legitimate emails appropriately.

Although rule-based training resulted in higher scores on the email identification test immediately after training, individuals who received rule-based training had similar test scores to those who received the control training after the 10-week period. Similar to mindfulness training, this finding implies that the benefits of rule-based training are short-term and that individuals who receive rule-based training will need to take refresher courses to maintain their resistance to phishing attacks. Even so, investing these resources into rule-based training may not valuable overall. In general, individuals who received rule-based training were no better at discriminating between legitimate and phishing emails or becoming less susceptible to phishing attacks compared to those who received the control training. Although previous researchers (e.g., Kumaraguru et al., 2007b; Sheng et al., 2010) found that receiving anti-phishing training resulted in better identification of phishing emails compared to receiving no anti-phishing training, Jensen et al. (2017) argued that receiving additional rule-based training may not yield additional benefits due to the desensitization of many rules and cues being repeated. For example, even without being provided rule-based training, individuals likely already know that they should not interact with emails sent from people they do not know and should not click on links that look highly suspicious or irrelevant to the email source. Thus, receiving rule-based training may not contribute much to one's existing knowledge of rules and cues associated with phishing emails and may even lead to

individuals taking the training less seriously and feeling overconfident in their capability to identify phishing emails (Kumaraguru et al., 2007b). Rather than using resources to implement rule-based training, it may be more advantageous to invest in other types of anti-phishing training—mindfulness training in particular—that yield more beneficial results.

Additionally, SDT analyses revealed that individuals who received mindfulness training were significantly more cautious to phishing on the email identification test immediately after training and maintained this level of caution throughout the 10-week period, indicated by similar negative values of *c* at both Time 1 and Time 2. However, it is important to note that individuals who received rule-based training or the control training also became significantly more cautious of phishing between Time 1 and Time 2. This significant change in response bias for the rule-based and control training groups may not be due to the training received (or lack thereof) but instead may simply be a function of participating in the study. In other words, within the 10-week period, participants were exposed to two rounds of mock phishing attacks, with the second round occurring 1 week before the second email identification test. This, along with other potential threats to internal validity (discussed in the study limitations), may have resulted in increased caution towards phishing. Even so, it is important to remember that this increase in caution is independent from one's capability to actually discriminate between legitimate and phishing emails. Thus, even though individuals who received the rule-based training or control training became more cautious of phishing over time, their capability to discriminate between legitimate and phishing emails was still significantly lower than individuals who received mindfulness training.

Overlearning on Phishing Identification and Susceptibility

Although previous research has shown that overlearning may be beneficial for retention, the majority of studies have only examined overlearning using simple laboratory tasks (e.g., verbal recall tasks) and within short retention intervals (e.g., less than 1 month; Craig et al., 1972; Krueger, 1929; Postman, 1963; Rohrer et al., 2005). In general, these studies found that the effects of overlearning quickly diminish over time and may only be beneficial for short-term retention. The present study addressed these limitations by examining overlearning with a more complex, real-world task (i.e., email identification task) over a longer retention interval (i.e., 2 months). The results showed that overlearning does not seem to yield any significant benefits in terms of helping individuals better discriminate between legitimate and phishing emails. In other words, receiving additional practice during training did not result in better test scores on the email identification tests and also did not result in significantly better retention in scores across the 10-week period.

Although these results suggest that overlearning on an email identification task may not be needed, receiving additional practice may still be valuable in terms of increasing individuals' caution towards phishing. SDT analyses revealed that individuals who received 100% overlearning were much more cautious of phishing when taking the email identification tests compared to those who did not receive overlearning. This is also consistent with the finding that individuals who received 100% overlearning scored better on the tests of vulnerability to mock phishing attacks. Because individuals who received overlearning were much more cautious of phishing, it is not surprising that they were also less likely to fall for phishing emails they received

throughout the study by erring on the side of caution and not clicking on any email links. Although overlearning was useful such that it increased caution towards phishing and essentially protected individuals from falling for phishing attacks, being increasingly cautious of phishing in and of itself has its own limitations. As stated by Kumaraguru et al. (2010), "…good security education should not only increase users' caution towards phishing but also teach them how to distinguish threats from non-threats" (p. 25). If overlearning only makes individuals more cautious of phishing but does not actually help them learn how to discriminate between legitimate and phishing emails, individuals will just label all emails they receive as phishing. Although false positives are much more favorable than false negatives or misses due to the severe consequences associated with falling for phishing attacks, being overly cautious can still disrupt individuals' work productivity if important emails are ignored.

The results also show that the effects of training do not differ as a function of overlearning, which is not too surprising considering how the desired outcomes of anti-phishing training and overlearning do not align. For example, to better protect individuals from phishing attacks, anti-phishing training should aim to promote System 2 thinking through conscious and deliberate information processing and allocation of necessary attention and effort when processing emails (Petty & Cacioppo, 1986; Stanovich & West, 2000; Vishwanath et al., 2011). However, overlearning works against this goal by promoting System 1 thinking. By providing additional practice and feedback on the same task, overlearning can lead to responses that are more automatic and require less attentional capacity (Arthur et al., 1998; Wang et al., 2013). Because a level of generalizability is required for email evaluation due to the variability in the

types of emails received, incorporating overlearning as a retention strategy into anti-phishing training may not be beneficial (or even logical) because the two strategies have competing intentions. In fact, if the intent of anti-phishing training is to better protect individuals against phishing attacks, overlearning may actually be counterproductive. In general, the effects of training were much more robust compared to the effects of overlearning. Thus, rather than focusing on the amount of practice provided during training, attention should instead be directed towards providing training—mindfulness training for instance—that achieves both goals of better email discriminability and increased caution towards phishing.

Practical Implications

Within recent years, phishing attacks have become increasingly prevalent and problematic. For example, in 2014, the Sony data breach resulted in the theft of an estimated 100 terabytes of data and, subsequently, the leak of sensitive employee and company information (Alvarez, 2014). Additionally, the 2017 Google Docs phishing attack affected an estimated 1 million Gmail users within just 1 hour and demonstrated how sophisticated and convincing these attacks have become (Warren, 2017). As phishing continues to be an increasingly common issue in society, it seems imperative for organizations to implement anti-phishing training to protect their employees and their organization as a whole from these devastating attacks. Although it should ultimately be the responsibility of individuals to educate themselves about the dangers of phishing, it is known that individuals are often overconfident in their capability to protect themselves against security-related attacks, are not motivated to learn about security, and treat security as a secondary task (Evers, 2006; Kumaraguru et al., 2007;

Nielsen, 2004). Thus, this can leave the burden upon organizations to educate their employees about the dangers of phishing, especially because they themselves are at risk if their employees fall for a phishing attack that compromises the entire organizational system. However, despite how contemporary media often only reports major phishing attacks or data breaches occurring in organizations, phishing attacks are not just isolated to these events. Phishers can and will continue to target individuals across all facets of life, which leaves anyone who uses email for personal-, school-, or work-related matters at risk of being a victim of a phishing attack. In particular, high school and college students are an especially vulnerable age group (Kumaraguru et al., 2009; Sheng et al., 2010), which implies that academic institutions also need to consider providing anti-phishing training to their students as well. By training these students early in their education, they will not only become more resistant to phishing attacks but will also be more prepared in handling phishing emails when they enter the workforce and join their respective organizations. In this regard, the broader organizational context in which anti-phishing training occurs also needs to be considered to maximize training effectiveness (Salas & Cannon-Bowers, 2000; Salas, Tannenbaum, Kraiger, & Smith-Jentsch, 2012). Because training motivation may likely already be low, it is essential for training facilitators, as well as organizational or institutional leaders, to communicate the importance and relevance of anti-phishing training to their employees, show continued support for the training, and reward good security-related behaviors. A broader organizational mindset of cybersecurity will not only motivate individuals to take anti-phishing training more seriously but it will also foster a transfer climate that will facilitate the use of knowledge and skills gained from anti-phishing training.

The results from this study also show that anti-phishing training does not require extensive resources to be an effective mechanism in terms of helping individuals learn how to discriminate between legitimate and phishing emails and become less susceptible to phishing attacks. Rather than distributing security information or notices for individuals to read on their own (which has been shown to be ineffective; Kumaraguru et al., 2007b), it seems that teaching individuals broadly about what phishing is, as well as specific strategies to utilize when evaluating emails (e.g., mindfulness techniques), and then providing opportunities for them to practice the skills learned and receive feedback can help individuals become more resistant to phishing attacks. Because the training was developed with simple slides containing text and graphics, organizations and academic institutions can easily implement similar anti-phishing training programs and reach a large number of employees and students quickly and efficiently via internet delivery.

It is important to note, however, that providing anti-phishing training will not eliminate all instances of phishing attacks. Despite receiving either rule-based or mindfulness training, 64% of participants still fell for at least one mock phishing email. Although clicking on a link within a mock phishing email does not imply that individuals would ultimately have given away their personal credentials if prompted on a fictitious website, it can still be argued that these individuals are vulnerable to phishing attacks by deciding to interact with these email messages. Additionally, it is unknown what potentially dangerous content phishers may include within these malicious links. As mentioned previously, training is only one strategy for combating phishing attacks and should be used in conjunction with better automated tools that

filter and warn individuals of these messages to maximize protection against phishing attacks (Hong, 2012). For organizations or individuals that do not have the resources for or access to advanced technological tools, training becomes especially important to defend against phishing attacks.

Although the results show the beneficial effects of incorporating overlearning during training to make individuals more cautious of phishing and, in turn, less likely to click on phishing emails, it should be cautioned that individuals must also be trained to discriminate between legitimate and phishing emails to not reduce work productivity. For example, if individuals are overly cautious to the extent that they are afraid of clicking on any links embedded in emails, they may ignore important, time-sensitive requests within their emails. In fact, Anandpara, Dingman, Jakobsson, Liu, and Roinestad (2007) noted that some anti-phishing educational resources only increase fear or concern in phishing and do not help individuals become any better at correctly identifying phishing emails. The results do not imply that providing individuals with increased practice during training should not be done but instead should be complemented with training that allows individuals to learn how to better discriminate between legitimate and phishing emails (e.g., mindfulness training).

Limitations and Future Research

There are several limitations that must be considered when interpreting and applying the results of the present study. First, the longitudinal nature of the study is subject to threats to internal validity such as history effects. For example, participants may have learned more about phishing on their own or been exposed to phishing-related information during the 10-week period. In this vein, participants likely received other

phishing emails that were not connected to the study and essentially had the opportunity to practice their email identification skills through their everyday email usage. Although all mock phishing emails included in the study were based on real-world examples of legitimate and phishing emails and were designed specifically to be relevant to the study sample (i.e., all emails came from known university sources or were related to the university), some emails may still have been more relevant to some participants versus others. Additionally, due to the proximity of participants being in similar classes, it is possible that participants across study conditions communicated with one another throughout the study to discuss their experiences. For example, although participants were not informed of the true nature of the mock phishing emails they received (i.e., they were led to an error page if they clicked on the embedded link), it is still possible that participants noticed a pattern during the two rounds of mock phishing attacks and warned others about these emails. As mentioned previously, individuals who received rule-based or the control training may have been more influenced by these effects compared to those who received mindfulness training, particularly in terms of caution towards phishing. As seen in Figure 8, individuals who received rule-based or the control training had a significant increase in caution towards phishing between Time 1 and Time 2, indicated by their positive values of *c* at Time 1 and negative values of *c* at Time 2. In fact, at Time 2, the level of caution towards phishing for these two training conditions was similar to the level of caution for those who received mindfulness training, who already became more cautious of phishing immediately after training and retained this level of caution from Time 1 to Time 2.

Second, to avoid practice effects and inducing increased levels of suspicion in participants regarding mock phishing emails, this study only administered tests at two time points (i.e., 1 week and 8 weeks after training for the tests of vulnerability to mock phishing attacks; 1 week and 10 weeks after training for the email identification tests). Because the study design did not allow for pre-tests to be conducted on the email identification tests and tests of vulnerability to mock phishing attacks (i.e., participants had to consent to participating in the study before any testing could be conducted), a large number of measures (e.g., prior phishing identification experience) were included in the study as covariates. However, conducting pre-tests would have provided greater insight regarding whether there were actual changes in test scores after training. Although the present study does include a longer retention interval compared to other studies examining anti-phishing training and overlearning, future research should consider extending the length of the experimental window and including additional time points. Examining more data points would give a clearer view of anti-phishing training skill retention trends or trajectories and provide greater insight regarding optimal time points for conducting training interventions (e.g., refresher courses).

Third, although Jensen et al. (2017) noted how mindfulness training should be supplemental to, rather than independent from, rule-based training, this study did not manipulate a combined rule-based and mindfulness training condition. Because rule-based training is the type of anti-phishing training that is commonly used and is assumed to be what most individuals are familiar with, it is not surprising that the effects of rule-based training were similar to those of the control training. Thus, future research should not only compare the effectiveness of rule-based and mindfulness

training as two distinct types of trainings but also include a combined rule-based and mindfulness training to determine whether learning rules and cues associated with phishing emails, as well as mindfulness techniques to apply when evaluating emails, results in even greater protection against phishing attacks.

Fourth, the amount of overlearning that was manipulated in this study (i.e., 100% overlearning) may not be the optimal amount for this type of task. Because no prior studies have examined overlearning within the context of anti-phishing training, the amount of overlearning used in the present study was determined based on previous research on overlearning that utilized other types of tasks. Due to the small effects of overlearning found in the present study, it is possible that 100% overlearning was not a sufficient amount needed to help individuals better discriminate between legitimate and phishing emails. Thus, future research should compare the effectiveness of other amounts of overlearning (e.g., 150% and 200% overlearning) to determine if there is an optimal amount of overlearning needed to help individuals become less susceptible to phishing attacks and retain their knowledge and skills gained from training.

Finally, this study only examined phishing attacks that requested individuals to click on embedded links within the mock phishing emails. Although email links are the most commonly used type of phishing method, phishing attacks extend far beyond these links and can include other requests such as downloading attachments, entering personal credentials onto fictitious websites, or responding to emails with sensitive or confidential information. Although the anti-phishing training provided in this study also taught individuals to be aware of attack methods beyond links, future research should examine the effectiveness of anti-phishing training and overlearning in terms of

becoming less susceptible to other types of phishing attacks. In this vein, future research should also examine how anti-phishing training and overlearning differs in effectiveness as a function of email content. In other words, various phishing influence tactics may be more or less effective as a result of anti-phishing training and overlearning. For example, some forms of phishing (e.g., spear phishing) are much more customized such that they incorporate personal information about the user in the email message or come from well-known sources with whom the user interacts, making the message much more persuasive compared to generic phishing emails that are mass distributed and are often irrelevant or not applicable to all users.

Conclusion

In summary, the results of the present study suggest that compared to anti-phishing training that emphasizes common rules and cues associated with phishing, anti-phishing training that incorporates mindfulness techniques is more beneficial in terms of helping individuals better discriminate between legitimate and phishing emails, become more cautious of phishing, and become less susceptible to phishing attacks. Although individuals who received mindfulness training did experience skill decay in their capability to discriminate legitimate and phishing emails across a 2-month period, these individuals were able to maintain their level of caution towards phishing and resistance to phishing attacks. Additionally, the beneficial effects of mindfulness training do not differ as a function of overlearning and were found to be much more influential compared to the independent effects of overlearning, which only resulted in increased caution towards phishing and less susceptibility to phishing attacks. Thus, rather than focusing on including additional practice during anti-phishing training,

attention should instead be directed towards teaching individuals how to withhold immediate judgment or action on email messages, critically evaluate and consider any requests being made, and check with a third-party source to verify the status of a message.

References

Abbasi, A., Zahedi, F., and Kaza, S. (2012a). Detecting Fake Medical Web Sites Using Recursive Trust Labeling. *ACM Transactions on Information Systems*, 30(4), 1-36.

Abbasi, A., Zahedi, F. M., and Chen, Y. (2012b). Impact of anti-phishing tool performance on attack success rates. *Proceedings of the IEEE International Conference on Intelligence and Security Informatics*, (pp. 12-17). Arlington, VA: IEEE.

Alnajim, A., & Munro, M. (2009, April). An evaluation of users' anti-phishing knowledge retention. Proceedings of the 2009 International Conference on *Information Management and Engineering,* (pp. 210-214). IEEE.

Alvarez, E. (2014). Sony Pictures hack: The whole story. Retrieved from https://www.engadget.com/2014/12/10/sony-pictures-hack-the-whole-story/

Anandpara, V., Dingman, A., Jakobsson, M., Liu, D., & Roinestad, H. (2007). Phishing IQ tests measure fear, not ability. In *International Conference on Financial Cryptography and Data Security* (pp. 362-366). Springer: Berlin, Heidelberg.

Anti-Phishing Working Group. Phishing Activity Trends Report, 4th Quarter 2016. February, 2017. http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf.

Arthur Jr., W., Bennett Jr., W., Stanush, P. L., & McNelly, T. L. (1998). Factors that influence skill decay and retention: A quantitative review and analysis. *Human Performance*, *11*(1), 57-101.

Baer, R. A. (2003). Mindfulness training as a clinical intervention: A conceptual and empirical review. *Clinical psychology: Science and Practice*, *10*(2), 125-143.

Baer, R. A., Smith, G. T., & Allen, K. B. (2004). Assessment of mindfulness by self-report: The Kentucky inventory of mindfulness skills. *Assessment*, *11*(3), 191-206.

Brown, K. W., Ryan, R. M., & Creswell, J. D. (2007). Mindfulness: Theoretical foundations and evidence for its salutary effects. *Psychological Inquiry*, *18*(4), 211-237.

Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying phishing susceptibility for detection and behavior decisions. *Human Factors*, *58*(8), 1158-1172.

Cialdini, R. B. (2009) Influence: Science and practice (5th ed.). Glenview, IL: Scott-Foresman.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, *19*(2), 189-211.

Craig, C. S., Sternthal, B., & Olshan, K. (1972). The effect of overlearning on retention. *Journal of General Psychology*, *87*, 86-94.

Dhamija, R., Tygar, J. D., and Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, (pp. 581-590). New York, NY: ACM.

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*, (pp. 79-90). New York, NY: ACM.

Driskell, J. E., & Johnston, J. H. (1998). Stress exposure training. In J. A. Cannon-Bowers, & E. Salas (Eds.), *Making decisions under stress: Implications for individual and team training* (pp. 191-217). Washington, DC: APA Press.

Driskell, J. E., Willis, R. P., & Copper, C. (1992). Effect of overlearning on retention. *Journal of Applied Psychology*, *77*(5), 615-622.

Everard, A., & Galletta, D. F. (2005). How presentation flaws affect perceived site quality, trust, and intention to purchase from an online store. *Journal of Management Information Systems*, *22*(3), 55-95.

Evers, J. (2006). User education is pointless. Retrieved from https://www.cnet.com/news/security-expert-user-education-is-pointless/.

Fitts, P. M. (1965). Factors in complex skill training. In R. Glaser (Ed.), *Training research and education* (pp. 177-197). New York: Wiley.

Goldberg, L. R. (1992). The development of markers for the big-five factor structure. *Psychological Assessment*, *4*(1), 26-42.

Grazioli, S., and Jarvenpaa, S. L. (2000). Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, 30(4), 395-410.

Green, D. M., & Swets, J. A. (1966). *Signal detection theory and psychophysics*. New York: Wiley.

Grossman, P., Niemann, L., Schmidt, S., & Walach, H. (2004). Mindfulness-based stress reduction and health benefits: A meta-analysis. *Journal of Psychosomatic Research*, *57*(1), 35-43.

Herzberg, A., and Jbara, A. (2008). Security and identification indicators for browsers against spoofing and phishing attacks. *ACM Transactions on Internet Technology*, 8(4), 1-45.

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

Hulsheger, U. R., Alberts, H. J. E. M., Feinholdt, A., & Lang, J. W. B. (2013). Benefits of mindfulness at work: The role of mindfulness in emotion regulation, emotional exhaustion, and job satisfaction. *Journal of Applied Psychology*, *98*(2), 310-325.

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

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.

Juola, J. F., & Hergenhahn, B. R. (1967). Probability matching and the overlearning reversal effect. *Psychonomic Science*, *8*, 309-310.

Karumbaiah, S., Wright, R. T., Durcikova, A., & Jensen, M. L. (2016). Phishing training: A preliminary look at the effects of different types of training. Proceedings of the 11th Pre-ICIS Workshop on Information Security and Privacy (pp. 1-10).

Kratzig, G. P. (2016). *Skill retention: A test of the effects of overlearning and skill retention interval on maintenance of infrequently used complex skills* (Unpublished doctoral dissertation). University of Regina, Regina, Saskatchewan.

Krueger, W. C. F. (1929). The effect of overlearning on retention. *Journal of Experimental Psychology*, *12*(1), 71-78.

Krueger, W. F. C. (1930). Further studies in overlearning. *Journal of Experimental Psychology*, *13*(2), 152.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish: A real-world evaluation of anti-phishing training. *SOUPS'09: Proceedings of the 5th Symposium on Usable Privacy and Security*. New York, NY: ACM.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L., Hong, J. and Nunge, E. (2007a). Protecting people from phishing: The design and evaluation of an embedded training email system. *CHI'07: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, (pp. 905-14). New York, NY: ACM.

Kumaraguru, P., Rhee, Y., Hasan, S., Acquisti, A., Cranor, L. and Hong, J. (2007b). Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. *Proceedings of the APWG 2nd Annual eCrime Researchers Summit*, (pp. 70-81). New York, NY: ACM.

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.

Lopez, M. A. (1980). Social-skills training with institutionalized elderly: Effects of precounseling structuring and overlearning on skill acquisition and transfer. *Journal of Counseling Psychology*, *27*(3), 286-293.

Macmillan, N. A., & Creelman, C. D. (1990). Response bias: Characteristics of detection theory, threshold theory, and "nonparametric" indexes. *Psychological Bulletin*, *107*(3), 401-413.

Macmillan, N. A., & Creelman, C. D. (2004). *Detection theory: A user's guide*. New York, NY: Psychology Press.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336-355.

Mandler, G. (1954). Transfer of training as a function of degree of response overlearning. *Journal of Experimental Psychology*, *47*(6), 411.

Mayhorn, C. B., & Nyeste, P. G. (2012). Training users to counteract phishing. *Work*, *41*, 3549-3552.

McCabe, J. (2016). FBI warns of dramatic increase in business e-mail scams. Retrieved from https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-dramatic-increase-in-business-e-mail-scams.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, *13*(3), 334-359.

Melnick, M. (1971). Effects of overlearning on the retention of a gross motor skill. *Research Quarterly*, *42*, 60-69.

Mitnick, K., & Simon, W. L. (2002). The art of deception: Controlling the human element of security. New York: Wiley.

Myers, S. (2007). Introduction to phishing. In M. Jakobsson & S. Myers (Eds.), Phishing and countermeasures: Understanding the increasing problem of electronic identity theft (pp. 1-29). Hoboken, NJ: Wiley.

Nielsen, J. (2004). User education is not the answer to security problems. Retrieved from https://www.nngroup.com/articles/security-and-user-education/.

Noe, R. A., & Schmitt, N. (1986). The influence of trainee attitudes on training effectiveness: Test of a model. *Personnel Psychology*, *39*(3), 497-523.

Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. *Advances in Experimental Social Psychology*, *19*, 123-205.

Purkait, S. (2012). Phishing counter measures and their effectiveness – literature review. *Information Management & Computer Security*, *20*(5), 382-420.

Rohrer, D., & Taylor, K. (2006). The effects of overlearning and distributed practice on the retention of mathematics knowledge. *Applied Cognitive Psychology*, *20*, 1209-1224.

Rohrer, D., Taylor, K., Pashler, H., Wixted, J. T., & Cepeda, N. J. (2005). The effect of overlearning on long-term retention. *Applied Cognitive Psychology*, *19*(3), 361-374.

Salas, E., & Cannon-Bowers, J. A. (2001). The science of training: A decade of progress. *Annual Review of Psychology*, *52*(1), 471-499.

Salas, E., Tannenbaum, S. I., Kraiger, K., & Smith-Jentsch, K. A. (2012). The science of training and development in organizations: What matters in practice. *Psychological Science in the Public Interest*, *13*(2), 74-101.

Schendel, J. D., & Hagman, J. D. (1982). On sustaining procedural skills over a prolonged retention interval. *Journal of Applied Psychology*, *67*, 605-610.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness

of interventions. CHI'10: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373-382). New York, NY: ACM.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. Paper presented at the Symposium On Usable Privacy and Security (SOUPS) 2007, Pittsburgh, PA, USA.

Stanovich, K. E., & West, R. F. (2000). Advancing the rationality debate. *Behavioral and Brain Sciences*, *23*(5), 701-717.

Swets, J. A., Dawes, R., & Monahan, J. (2000). Psychological science can improve diagnostic decisions. *Psychological Science in the Public Interest*, *1*(1), 1-26.

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, X., Day, E. A., Kowollik, V., Schuelke, M. J., & Hughes, M. G. (2013). Factors influencing knowledge and skill decay after training: A meta-analysis. In W. Arthur, Jr., E. A. Day, W. Bennett, Jr., & A. Portrey (Eds.), *Individual and team skill decay: State of the science and implications for practice* (pp. 68-116). New York: Taylor-Francis.

Warren, T. (2017). Google has fixed the massive Google Docs phishing attack. Retrieved from https://www.theverge.com/2017/5/3/15537064/google-docs-phishing-attack-fixed.

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance. *Information systems research*, *25*(2), 385-400.

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.

Zhang, Y., Egelman, S., Cranor, L., & Hong, J. (2007). Phinding Phish: Evaluating Anti-Phishing Tools. *Proceedings of the 14th Annual Network and Distributed System Security Symposium*.

Table 1

Summary of Study Hypotheses and Research Questions and Associated Support Found

Hypothesis/Research Question	Description	Type of Test	Results
Hypothesis 1	Individuals who receive either rule-based training or mindfulness training will be **a) better at identifying phishing emails** and **b) less vulnerable to phishing attacks in their everyday email use** compared to individuals who do not receive anti-phishing training.	Main effect of training of **a) scores on the email identification tests** and **b) scores on the tests of vulnerability to mock phishing attacks**	Hypothesis 1a supported: training > no training Hypothesis 1b not supported: training = no training
		Supplemental SDT analyses	
		Main effect of training of discriminability (*d'*)	*d'*: training = no training
		Main effect of training of response bias (*c*)	*c*: training = no training
Hypothesis 2	Individuals who receive mindfulness training will be **a) better at identifying phishing emails** and **b) less vulnerable to phishing attacks in their everyday email use** compared to individuals who receive rule-based training.	Main effect of training of **a) scores on the email identification tests** and **b) scores on the tests of vulnerability to mock phishing attacks**	Hypotheses 2a and 2b supported: mindfulness training > rule-based training
		Supplemental SDT analyses	
		Main effect of training of **discriminability (*d'*)**	*d'*: mindfulness > rule-based
		Main effect of training of **response bias (*c*)**	*c*: mindfulness = rule-based

Note. SDT = Signal Detection Theory

Table 1 Continued

Hypothesis/Research Question	Description	Type of Test	Results
Hypothesis 3	Individuals who receive mindfulness training will have greater retention 2 months after training in terms of **a) identifying phishing emails** and **b) being less vulnerable to phishing attacks in their everyday email use** compared to individuals who receive rule-based training.	*Amount of retention/decay* 2 (training method: rule-based or mindfulness) × 2 (test administration: Time 1 and Time 2) ANCOVA on the **a) scores on the email identification tests** and **b) scores on the tests of vulnerability to mock phishing attacks**	*Amount of retention/decay* Hypothesis 3a and 3b not supported
		Sheer level of performance Main effect of training of **a) scores on the email identification test at Time 2** and **b) scores on the test of vulnerability to mock phishing attacks at Time 2**	*Sheer level of performance* Hypothesis 3a supported but Hypothesis 3b not supported
		Supplemental SDT analyses	
		Amount of retention/decay 2 (training: rule-based or mindfulness) × 2 (test administration: Time 1 and Time 2) ANCOVA on **discriminability (*d'*)**	*Amount of retention/decay* *d'*: mindfulness = rule-based
		2 (training: rule-based or mindfulness) × 2 (test administration: Time 1 and Time 2) ANCOVA on **response bias (*c*)**	*c*: rate of change for rule-based > mindfulness (i.e., became overly cautious)
		Sheer level of performance Main effect of training of **discriminability (*d'*) at Time 2**	*Sheer level of performance* *d'*: mindfulness > rule-based
		Main effect of training of **response bias (*c*) at Time 2**	*c*: mindfulness = rule-based

Note. SDT = Signal Detection Theory

Table 1 Continued

Hypothesis/Research Question	Description	Type of Test	Results
Research Question 1	How does overlearning during training affect the **a) identification of phishing emails** and **b) vulnerability to phishing attacks** 2 months after training is completed?	Main effect of overlearning of **a) scores on the email identification tests** and **b) scores on the tests of vulnerability to mock phishing attacks**	No statistically significant difference found for Research Question 1a; 100% overlearning = no overlearning Significant difference found for Research Question 1b; 100% overlearning > no overlearning
		Amount of retention/decay 2 (overlearning: 100% overlearning or no overlearning) × 2 (test administration: Time 1 and Time 2) ANCOVA on the **a) scores on the email identification tests** and **b) scores on the tests of vulnerability to mock phishing attacks**	*Amount of retention/decay*: No statistically significant differences found for Research Questions 1a and 1b; 100% overlearning = no overlearning
		Sheer level of performance Main effect of overlearning of **a) scores on the email identification test at Time 2** and **b) scores on the test of vulnerability to mock phishing attacks at Time 2**	*Sheer level of performance*: No statistically significant differences found for Research Questions 1a and 1b; 100% overlearning = no overlearning
		Supplemental SDT analyses Main effect of training of overlearning of **discriminability (*d'*)**	*d'*: 100% overlearning = no overlearning
		Main effect of training of overlearning of **response bias (*c*)**	*c*: 100% overlearning > no overlearning

Note. SDT = Signal Detection Theory

Table 1 Continued

Hypothesis/Research Question	Description	Type of Test	Results
		Amount of retention/decay 2 (overlearning: 100% overlearning or no mindfulness) × 2 (test administration: Time 1 and Time 2) ANCOVA on **discriminability (*d'*)**	*Amount of retention/decay* *d'*: 100% overlearning = no overlearning
		2 (overlearning: 100% overlearning or no mindfulness) × 2 (test administration: Time 1 and Time 2) ANCOVA on **response bias (*c*)**	*c*: 100% overlearning = overlearning
		Sheer level of performance Main effect of overlearning of **discriminability (*d'*) at Time 2**	*Sheer level of performance* *d'*: 100% overlearning = no overlearning
		Main effect of overlearning of **response bias (*c*) at Time 2**	*c*: 100% overlearning = no overlearning
Research Question 2	Are the effects of overlearning during training on the identification of phishing emails different for rule-based and mindfulness training 2 months after training is completed?	*Amount of retention/decay* 2 (training: rule-based or mindfulness) × 2 (overlearning: 100% overlearning or no overlearning) × 2 (test administration: Time 1 and Time 2) ANCOVA on the **a) scores on the email identification tests** and **b) scores on the tests of vulnerability to mock phishing attacks**	*Amount of retention/decay* No statistically significant differences found for Research Questions 2a and 2b
		Sheer level of performance 2 (training: rule-based or mindfulness) × 2 (overlearning: 100% overlearning or no overlearning) ANCOVA on the **a) scores on the email identification test at Time 2** and **b) scores on the test of vulnerability to mock phishing attacks at Time 2**	*Sheer level of performance* No statistically significant differences found for Research Questions 2a and 2b

Note. SDT = Signal Detection Theory

Table 1 Continued

Hypothesis/Research Question	Description	Type of Test	Results
		Supplemental SDT analyses	
		Amount of retention/decay 2 (training: rule-based or mindfulness) × 2 (overlearning: 100% overlearning or no overlearning) × 2 (test administration: Time 1 and Time 2) ANCOVA on **discriminability (*d'*)**	*Amount of retention/decay* *d'*: No statistically significant differences found
		2 (training: rule-based or mindfulness) × 2 (overlearning: 100% overlearning or no overlearning) × 2 (test administration: Time 1 and Time 2) ANCOVA on **response bias (*c*)**	*c*: No statistically significant differences found
		Sheer level of performance 2 (training: rule-based or mindfulness) × 2 (overlearning: 100% overlearning or no overlearning) ANCOVA on **discriminability (*d'*)**	*Sheer level of performance* *d'*: No statistically significant differences found
		2 (training: rule-based or mindfulness) × 2 (overlearning: 100% overlearning or no overlearning) ANCOVA on **response bias (*c*)**	*c*: No statistically significant differences found

Note. SDT = Signal Detection Theory

Table 2

Means, Standard Deviations, Reliabilities, and Correlations of Study Variables

Variable	*M*	*SD*	1	2	3	4	5	6	7	8
1. Disposition to trust[1]	5.05	1.18	(.87)							
2. Mindfulness in technology[1]	4.93	1.25	-.00	(.89)						
3. Perceived Internet risk[1]	4.67	1.14	-.05	.03	(.87)					
4. Computer self-efficacy - Internal[1]	3.65	1.24	-.02	.53	-.03	(.87)				
5. Computer self-efficacy - External[1]	5.90	0.91	.07	.35	-.02	.42	(.84)			
6. Phishing identification expertise[1]	4.33	1.39	-.06	.33	.02	.27	.17	(.85)		
7. Email experience[1]	5.50	0.99	.01	.22	.03	.18	.23	.17	(.88)	
8. Pre-training motivation[1]	6.07	0.90	.10	.24	.18	.11	.18	.10	.09	(.87)
9. Extraversion[2]	5.58	1.02	.09	.02	-.06	-.02	.07	-.09	.04	-.01
10. Conscientiousness[2]	6.69	0.82	.11	.05	-.03	-.00	.12	.05	.26	.20
11. Openness to learn[2]	6.48	0.92	-.01	.30	.01	.18	.23	.12	.11	.08
12. Emotional stability[2]	5.07	0.90	.02	.00	-.07	.14	.10	.11	.03	.08
13. Agreeableness[2]	7.09	0.79	.29	.08	.04	-.04	.17	-.07	.10	.18
14. Email Identification Test 1[3]	7.35	1.69	-.09	.02	-.07	.04	.14	.10	.06	.06
15. Email Identification Test 2[3]	7.02	1.61	.00	.09	-.10	.06	.10	.06	.10	.06
16. Mock Phishing Test 1[4]	4.26	1.00	-.02	-.01	.04	-.02	-.05	.00	-.01	.03
17. Mock Phishing Test 2[4]	4.41	0.83	.04	-.02	-.10	-.02	.01	-.01	.03	.06

Note. Diagonals are internal consistencies. [1] Variable measured on a 1-to-7 Likert Scale.
[2] Variable measured on a 1-to-9 Likert Scale. [3] Scores ranged between 0 to 10. [4]Scores ranged between 0 to 5.
$r > |.09| = p < .05$, $r > |.12| = p < .01$, $r > |.15| = p < .001$ (two-tailed); $N = 453$.

Table 2 Continued

Variable	9	10	11	12	13	14	15	16	17
1. Disposition to trust[1]									
2. Mindfulness in technology[1]									
3. Perceived Internet risk[1]									
4. Computer self-efficacy - Internal[1]									
5. Computer self-efficacy - External[1]									
6. Phishing identification expertise[1]									
7. Email experience[1]									
8. Pre-training motivation[1]									
9. Extraversion[2]	(.89)								
10. Conscientiousness[2]	.19	(.87)							
11. Openness to learn[2]	.24	.19	(.75)						
12. Emotional stability[2]	.15	.24	.00	(.84)					
13. Agreeableness[2]	.25	.40	.42	.26	(.79)				
14. Email Identification Test 1[3]	-.02	.03	.05	.05	.01	(.59)			
15. Email Identification Test 2[3]	.05	.07	.15	.07	.09	.24	(.28)		
16. Mock Phishing Test 1[4]	-.04	-.02	-.02	.04	-.05	.05	.04	(.49)	
17. Mock Phishing Test 2[4]	.06	-.02	-.01	-.03	.01	.14	.07	.24	(.29)

Note. Diagonals are internal consistencies. [1] Variable measured on a 1-to-7 Likert Scale.
[2] Variable measured on a 1-to-9 Likert Scale. [3] Scores ranged between 0 to 10. [4]Scores ranged between 0 to 5.
$r > |.09| = p < .05$, $r > |.12| = p < .01$, $r > |.15| = p < .001$ (two-tailed); $N = 453$.

Table 3

Results of Mixed Design Analysis of Covariance - Adjusted Means and Standard Errors by Study Conditions for Scores on Email Identification Tests at Time 1 and Time 2

		Time 1		Time 2	
Condition	*n*	*M*	*SE*	*M*	*SE*
Rule-Based Training, No Overlearning	81	6.93	.18	6.71	.18
Rule-Based Training, 100% Overlearning	77	7.76	.18	6.77	.18
Rule-Based Training Total	158	7.34	.13	6.74	.13
Mindfulness Training, No Overlearning	69	7.97	.19	7.41	.19
Mindfulness Training, 100% Overlearning	76	7.89	.18	7.55	.18
Mindfulness Training Total	145	7.93	.13	7.48	.13
Control Training, No Overlearning	72	6.77	.19	6.95	.19
Control Training, 100% Overlearning	78	6.84	.18	6.79	.18
Control Training Total	150	6.81	.13	6.87	.13
No Overlearning Total	222	7.22	.11	7.02	.11
100% Overlearning Total	231	7.50	.11	7.04	.10
Total	453	7.36	.08	7.03	.07

Note. Scores range from 0 to 10. Means were adjusted for external computer self-efficacy as a covariate.

Table 4

Results of Mixed Design Analysis of Covariance - Means and Standard Errors by Study Conditions for Scores on Tests of Vulnerability to Mock Phishing Attacks at Time 1 and Time 2

		Time 1		Time 2	
Condition	*n*	*M*	*SE*	*M*	*SE*
Rule-Based Training, No Overlearning	81	4.03	.11	4.26	.09
Rule-Based Training, 100% Overlearning	77	4.38	.11	4.38	.09
Rule-Based Training Total	158	4.20	.08	4.32	.07
Mindfulness Training, No Overlearning	69	4.41	.12	4.39	.10
Mindfulness Training, 100% Overlearning	76	4.50	.11	4.67	.09
Mindfulness Training Total	145	4.46	.08	4.53	.07
Control Training, No Overlearning	72	4.14	.12	4.40	.10
Control Training, 100% Overlearning	78	4.15	.11	4.36	.09
Control Training Total	150	4.15	.08	4.38	.07
No Overlearning Total	222	4.19	.07	4.35	.06
100% Overlearning Total	231	4.34	.07	4.47	.05
Total	453	4.27	.05	4.41	.04

Note. Scores range from 0 to 5. There were no statistically significant covariates for scores on tests of vulnerability to mock phishing attacks.

Table 5

Results of Mixed Design Analysis of Covariance Predicting Scores for Email Identification Tests at Time 1 and Time 2

Source	*df*	Mean Square	*F*	η_p^2
Within-Person				
Time	1	0.25	0.06	.00
Time × Training	2	18.60	4.60*	.02
Time × Overlearning	1	7.71	1.91	.00
Time × Training × Overlearning	2	9.44	2.33	.01
Error	446	4.05		
Between-Person				
Covariates				
Computer self-efficacy - External	1	21.03	13.85***	.03
Effects				
Training	2	30.26	19.92***	.08
Overlearning	1	2.41	1.59	.00
Training × Overlearning	2	2.72	1.79	.01
Error	446	1.52		

Note. * $p < .05$, *** $p < .001$ (two-tailed). $N = 453$.

Table 6

Results of Mixed Design Analysis of Covariance Predicting Scores for Tests of Vulnerability to Mock Phishing Attacks at Time 1 and Time 2

Source	*df*	Mean Square	*F*	η_p^2
Within-Person				
Time	1	9.28	7.12**	.02
Time × Training	2	0.98	0.75	.00
Time × Overlearning	1	0.15	0.11	.00
Time × Training × Overlearning	2	1.67	1.28	.01
Error	447	1.30		
Between-Person				
Training	2	2.62	5.17**	.02
Overlearning	1	2.08	4.11*	.01
Training × Overlearning	2	0.66	1.31	.01
Error	447	0.51		

Note. * $p < .05$, ** $p < .01$ (two-tailed). $N = 453$.

Table 7

Results of Mixed Design Analysis of Covariance - Adjusted Means and Standard Errors by Study Conditions for d' on Email Identification Tests at Time 1 and Time 2

		Time 1		Time 2	
Condition	*n*	*M*	*SE*	*M*	*SE*
Rule-Based Training, No Overlearning	81	1.01	.10	0.86	.09
Rule-Based Training, 100% Overlearning	77	1.42	.10	0.89	.10
Rule-Based Training Total	158	1.22	.07	0.88	.07
Mindfulness Training, No Overlearning	69	1.52	.10	1.21	.10
Mindfulness Training, 100% Overlearning	76	1.47	.10	1.30	.10
Mindfulness Training Total	145	1.49	.07	1.26	.07
Control Training, No Overlearning	72	0.88	.10	0.99	.10
Control Training, 100% Overlearning	78	0.92	.10	0.90	.09
Control Training Total	150	0.90	.07	0.95	.07
No Overlearning Total	222	1.14	.06	1.02	.06
100% Overlearning Total	231	1.27	.06	1.03	.06
Total	453	1.20	.04	1.03	.04

Note. Means were adjusted for external computer self-efficacy as a covariate.

Table 8

Results of Mixed Design Analysis of Covariance - Means and Standard Errors by Study Conditions for c on Email Identification Tests at Time 1 and Time 2

		Time 1		Time 2	
Condition	*n*	*M*	*SE*	*M*	*SE*
Rule-Based Training, No Overlearning	81	.18	.05	-.06	.05
Rule-Based Training, 100% Overlearning	77	.00	.05	-.12	.05
Rule-Based Training Total	158	.09	.03	-.09	.03
Mindfulness Training, No Overlearning	69	-.02	.05	-.06	.05
Mindfulness Training, 100% Overlearning	76	-.08	.05	-.15	.05
Mindfulness Training Total	145	-.05	.03	-.10	.04
Control Training, No Overlearning	72	.12	.05	-.21	.05
Control Training, 100% Overlearning	78	.08	.05	-.15	.05
Control Training Total	150	.10	.03	-.18	.04
No Overlearning Total	222	.10	.03	-.11	.03
100% Overlearning Total	231	.00	.03	-.14	.03
Total	453	.05	.02	-.13	.02

Note. Means < 0 reflect erring on the side of treating emails as being phishing (i.e., greater caution towards phishing), whereas means > 0 reflect erring on the side of treating emails as legitimate (i.e., greater vulnerability). There were no statistically significant covariates for *c* on the email identification tests.

Table 9

Results of Mixed Design Analysis of Covariance Predicting d' on Email Identification Tests at Time 1 and Time 2

Source	*df*	Mean Square	*F*	η_p^2
Within-Person				
Time	1	0.03	0.02	.00
Time × Training	2	6.16	5.41**	.02
Time × Overlearning	1	1.75	1.53	.00
Time × Training × Overlearning	2	2.57	2.26	.01
Error	446	1.14		
Between-Person				
Covariates				
Computer self-efficacy - External	1	5.19	11.99**	.03
Effects				
Training	2	7.99	18.45***	.08
Overlearning	1	0.56	1.30	.00
Training × Overlearning	2	0.63	1.45	.01
Error	446	0.43		

Note. * $p < .05$, ** $p < .01$, *** $p < .001$ (two-tailed). $N = 453$.

Table 10

Results of Mixed Design Analysis of Covariance Predicting c on Email Identification Tests at Time 1 and Time 2

Source	*df*	Mean Square	*F*	η_p^2
Within-Person				
Time	1	13.58	47.20***	.10
Time × Training	2	1.93	6.70**	.03
Time × Overlearning	1	0.44	1.54	.00
Time × Training × Overlearning	2	0.26	0.89	.00
Error	447	0.29		
Between-Person				
Training	2	0.22	2.17	.01
Overlearning	1	0.46	4.62*	.01
Training × Overlearning	2	0.18	1.80	.01
Error	447	0.10		

Note. * $p < .05$, ** $p < .01$, *** $p < .001$ (two-tailed). $N = 453$.

Study Conditions / Study Procedures	Rule-based training, 100% overlearning	Mindfulness training, 100% overlearning	Control training, 100% overlearning	Rule-based training, No overlearning	Mindfulness training, No overlearning	Control training, No overlearning
Study Introduction & Pre-training measures	Informed consent Introduction to study Covariate measures[1]					
Training Manipulation	Rule-based training	Mindfulness training	Control Training	Rule-based training	Mindfulness training	Control training
Practice	Email Identification Practice (six emails)					
Overlearning Manipulation	Additional Practice (6 additional emails)	Additional Practice (6 additional emails)	Additional Practice (6 additional emails)	No additional practice	No additional practice	No additional practice
1st Email Identification Test & Post-training measures	Big Five personality measure Email identification test #1[2] Demographics Training debrief					
1st Round of Mock Phishing Attacks	**1 week after training session** Mock phishing attack test #1[3]					
2nd Round of Mock Phishing Attacks	**8 weeks after training session** Mock phishing attack test #2[3]					
2nd Email Identification Test	**10 weeks after training session[4]** Email identification test #2[2] Full study debrief					

Figure 1. General study procedures.

[1] Covariate measures included disposition to trust, mindfulness in technology, perceived Internet risk, computer self-efficacy, phishing identification expertise, email experience, web experience, and pre-training motivation.

[2] Email identification test #1 and #2 (10 emails each) were counterbalanced.

[3] Mock phishing attack test #1 and #2 (five emails each) were counterbalanced and distributed over a two-week period.

[4] Email identification test #2 was sent after the conclusion of mock phishing attack test #2 and was taken online instead of in-person as email identification test #1.

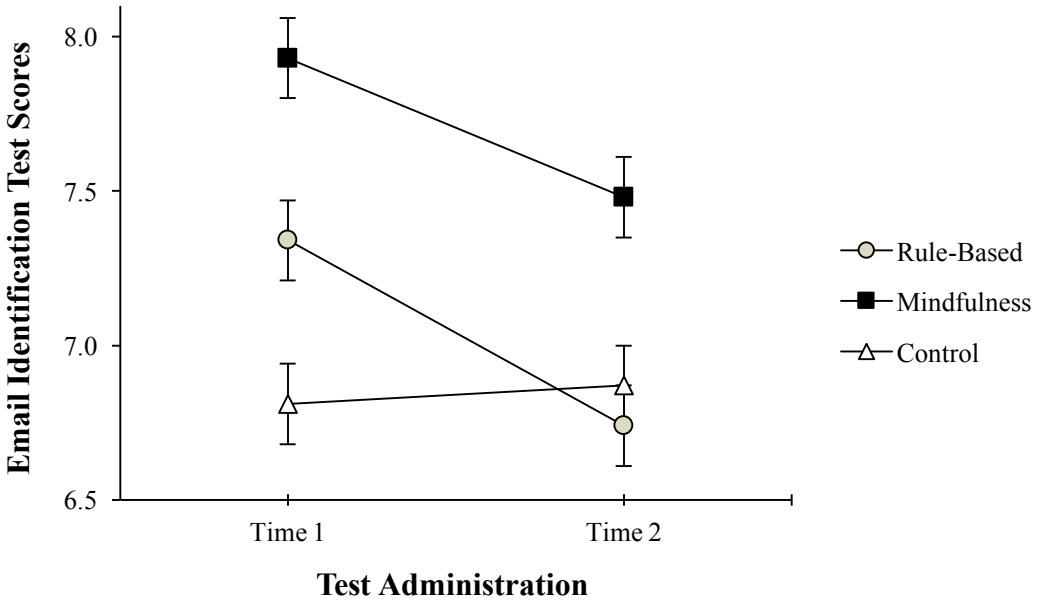


Figure 2. Interaction between training and test administration on email identification test scores. Higher scores indicate better performance. Error bars reflect one standard error.

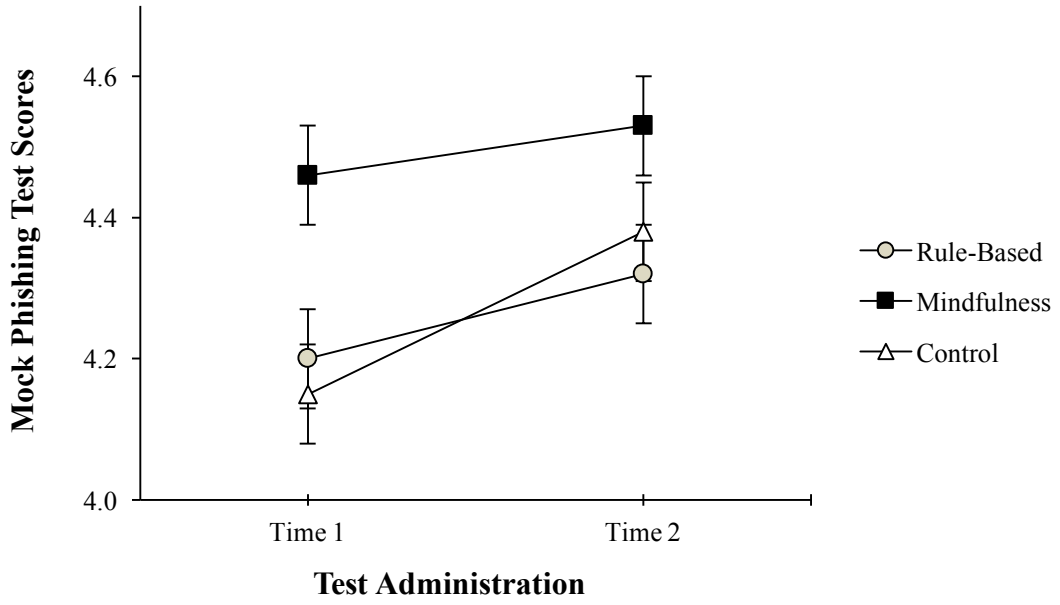


Figure 3. Effects of training and test administration on mock phishing test scores. Higher scores indicate better performance. Error bars reflect one standard error.

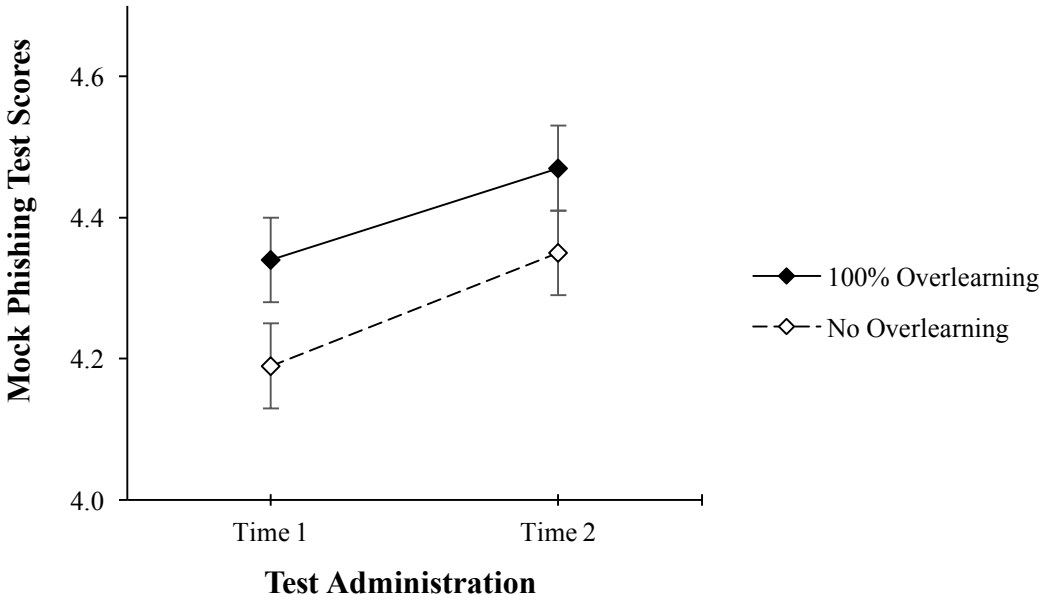


Figure 4. Effects of overlearning and test administration on mock phishing test scores. Higher scores indicate better performance. Error bars reflect one standard error.

		Signal (Type of Email)	
		Present (Phishing)	**Absent (Legitimate)**
"Is this a phishing message?"	**Yes**	Hit	False Positive
	No	Miss/False Negative	Correct Rejection

Figure 5. Signal detection theory response types in a phishing detection context.

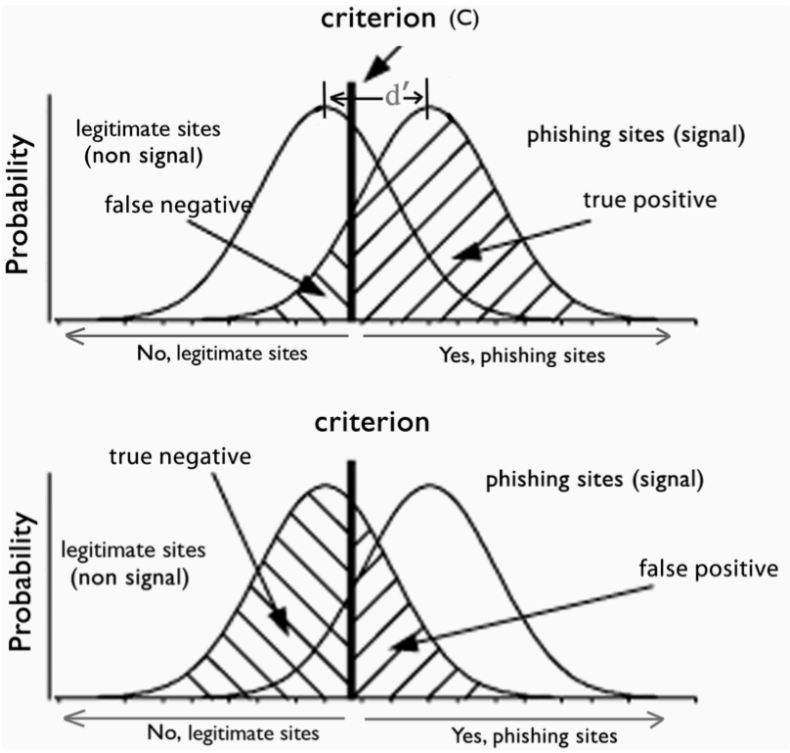


Figure 6. Signal detection theory distributions in a phishing detection context. From "Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish," by S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. Cranor, J. Hong, and E. Nuge, 2007, Proceedings of the 3rd Symposium on Usable Privacy and Security, 88-99. Copyright (2007) by Steve Sheng. Reprinted with permission.

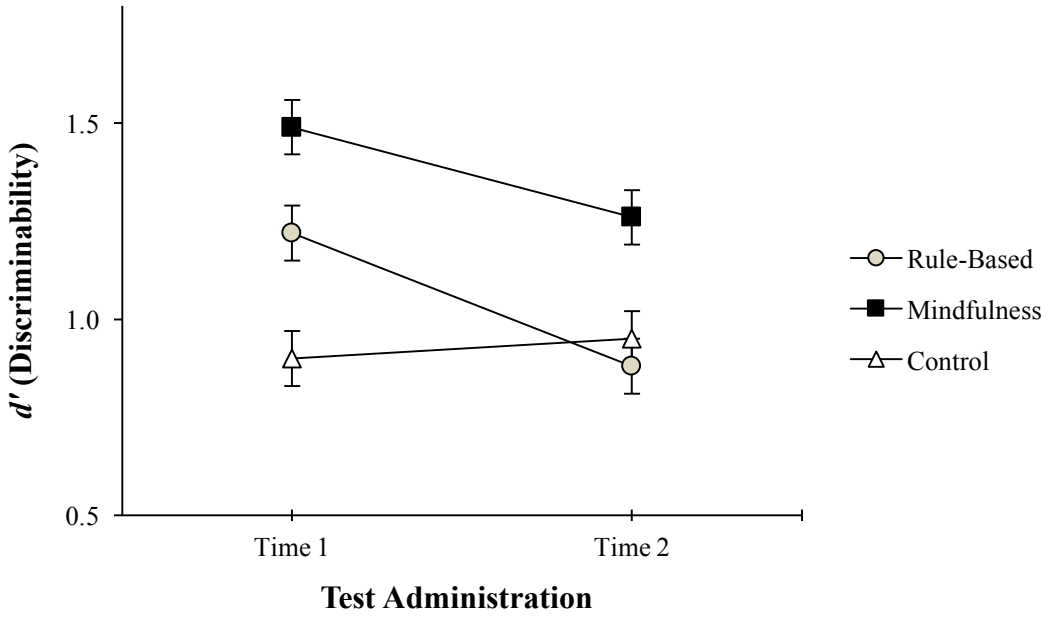


Figure 7. Interaction between training and test administration on *d'* (discriminability) for email identification tests. Higher scores indicate better performance. Error bars reflect one standard error.

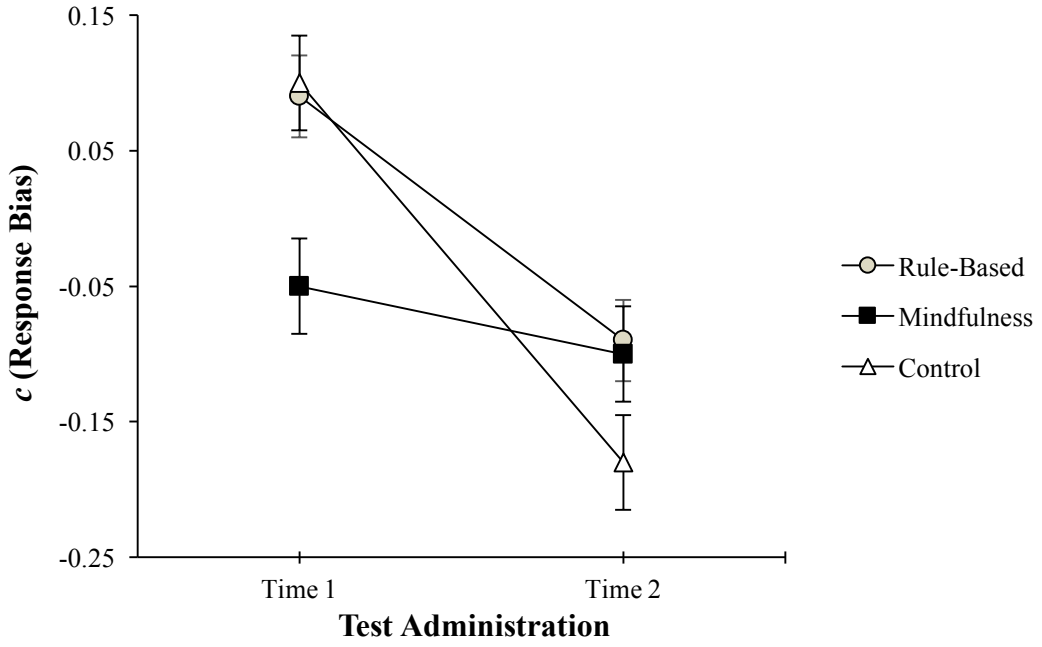


Figure 8. Interaction between training and test administration on *c* (response bias) for email identification tests. Negative scores reflect erring on the side of treating emails as being phishing (i.e., greater caution towards phishing), whereas positive values reflect erring on the side of treating emails as legitimate (i.e., greater vulnerability). Error bars reflect one standard error.

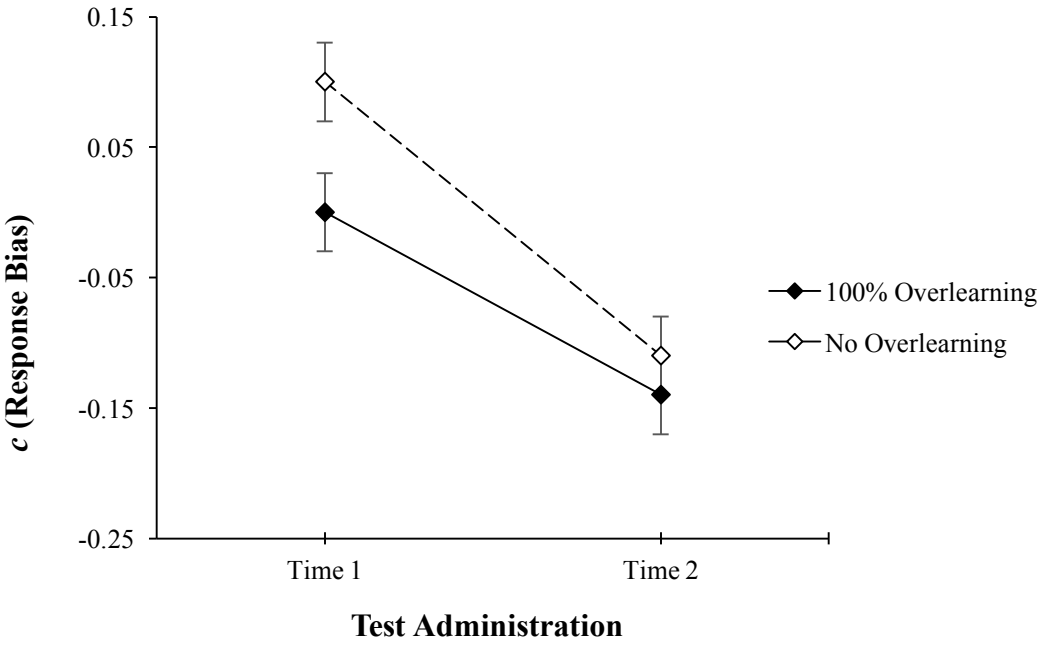


Figure 9. Effects of overlearning and test administration on *c* (response bias) for email identification tests. Negative scores reflect erring on the side of treating emails as being phishing (i.e., greater caution towards phishing), whereas positive values reflect erring on the side of treating emails as legitimate (i.e., greater vulnerability). Error bars reflect one standard error.

Appendix A: General Phishing Training Content

What is Phishing?

- Phishing is a method for stealing personal information, such as usernames and passwords, from Internet users by sending electronic messages that imitate or "spoof" a valid message

- Criminals use phishing to steal information by sending messages that mimic a trustworthy source

- A phisher may send you a message that will ask you to:
    - Open an attachment that will install something harmful on your computer
    - Click on a link to a harmful website
    - Reply to a message with your private information

- Phishing attacks can occur through email, instant messaging or texting, and social media

- Phishers may use influence techniques to get you to respond by trying to make you believe:
    - You and the phisher know each other and are friends
    - Others are responding and you should too
    - The response needed is time-sensitive
    - The request comes from someone who has legitimate authority such as a supervisor

How It Works

Phishing occurs in three phases:

1. **The Bait**
   - Phishers send emails to users asking them to click on a link, download or open an attachment, or respond to the email

2. **The Hook**
   - Users click on legitimate-looking websites that are set up only to capture sensitive information

3. **The Catch**
   - Phishers monetize the stolen information through activities such as fraud or identity theft

Why Should I Care?

- Phishing attacks on OU email accounts are at an all-time high
- More than 70% of phishing attacks are on university staff and students
- Most phishing attacks try to get information in order to steal from your accounts

Facts

- If you have an OU email address, **you are a target!**
- You probably have already received phishing emails!
- It is crucial that you understand how to recognize and react to phishing!

Appendix B: Password Management Training Content

Guidelines for Creating a Password

- Make it longer by using at least 12 characters
- Use passphrases (i.e., a string of words), not single passwords
- Choose three or four words that you can easily remember (e.g., horsesloveeatingapples)
- Add special characters that are easy to remember (e.g., 4horse$loveeating4apple$)

Guidelines for Creating a Password

- Always choose a unique password for every sensitive account (e.g., financial or work)
- Never reveal your password to anyone else
- Periodically change your password for sensitive accounts
- Do not use the “Remember Password” feature in your browser

If your OU password doesn’t meet the guidelines or if you haven’t changed your password in the past year, you should change your password!

Guidelines for Managing your Passwords

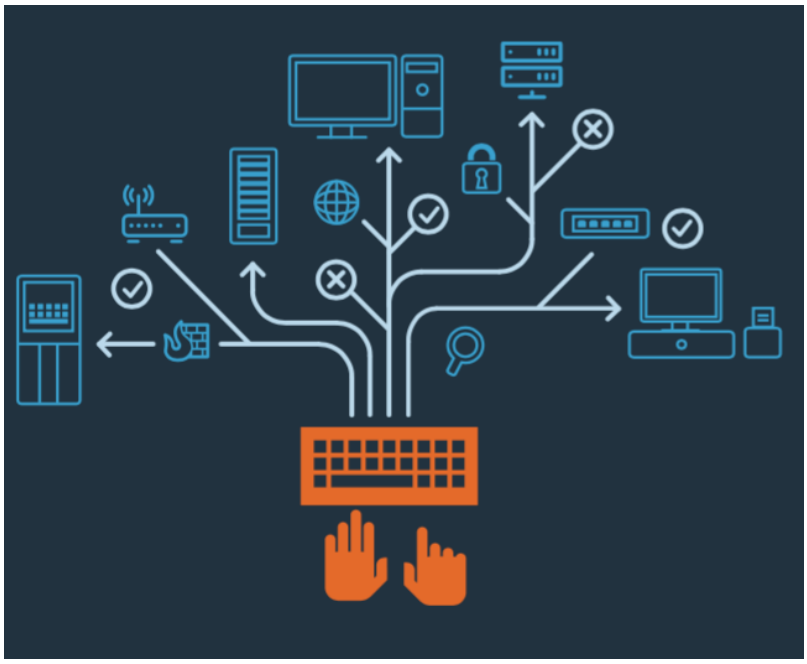
Option 1: Memorize passwords and don't keep a password copy for most sensitive accounts (financial, work)

- Ideal for password management
- Frequent use makes remembering easier

Option 2: Use a password vault to digitally store your passwords with strong encrytion

- Password vault is a software that stores passwords and is accessed by a single, long password
- Secure option for storing passwords to sensitive but rarely used accounts
- Access depends on remembering your vault password

Guidelines for Managing your Passwords



Option 3: Store a physical copy of your password in a secure location

- Much less secure than memorization or a vault but is a practical compromise for less sensitive accounts
- Example locations: locked cabinet or locked drawer
- Never leave passwords by your device or in plain view

If you feel your OU password has been compromised, change your password immediately by going to accounts.ou.edu. The OU IT Help Desk can be a valuable resource by contacting security@ou.edu.

Appendix C: Rule-Based Training Content

To avoid phishing, you need to carefully evaluate emails that you receive and look for cues that the email is phishing. **If you follow these six simple suggestions, you can avoid phishing attacks**:

1. Be suspicious of an email or website that asks for sensitive or private information
2. Never click on a link or open an attachment in an email from an unknown sender
3. Do not reply to emails asking for sensitive or private information
4. Real organizations such as banks or employers will never ask for sensitive or private information in an email
5. Access a website by typing the web address yourself
6. Hover over the link and look for cues such as 'https://' in the address bar (the 's' stands for secure) or a lock icon in your browser to distinguish between legitimate and fake addresses

Remember!

- Phishers want to steal your information and money
- They try to send emails that look legitimate by using a forged email address, adding fake links, and demanding private information
- They are hoping you overlook cues that give them away
- If you respond to these emails, if could cost you and OU!

If you have any questions, you can check the OU IT Help Desk at security@ou.edu.

Appendix D: Mindfulness Training Content

Whenever you get an email message that requests you to click on a link, download a file, or provide information, you should remember these three steps: **Stop, Think, and Check!**

1. **Stop**
   - Take a few minutes and do not mindlessly and immediately act on an email by clicking a link, downloading a file, or replying

2. **Think**
   - Consider for a moment what the email is requesting and ask yourself these four questions:
     - **Does the request ask for private or proprietary information?**
     - **Is the request unexpected or rushed?**
     - **Does the request make sense?**
     - **Why would the sender need me to do this?**

3. **Check**
   - If you have any questions about the email, comment the OU IT Help Desk at security@ou.edu.

Remember!

- Phishers want to steal your information and money
- They try to send emails that look legitimate by using a forged email address, adding fake links, and demanding private information
- They are hoping you overlook cues that give them away
- If you respond to these emails, if could cost you and OU!

If you have any questions, you can check the OU IT Help Desk at security@ou.edu.

Appendix E: Example Emails with Training Feedback

From "OU Email Admin" <donotreply@okstateuniversity.edu>
To: donotreply@okstateuniversity.edu
Subject: Email Account Update
Date: Thu, 2 Feb 2017 13:36:31 +0730

Dear OU Student,

Due to migration to a new Open Source Email Collaboration Solution (SunsetGates), it is mandatory that you update your OU information immediately by using the update link below.

Update here

Failure to update will result in closure of your account.

Thanks for your cooperation!
OU Email Admin Desk

Why is this a phishing email?

Feedback for rule-based training condition

- The sender's email address is unknown and not from OU
- The link is not secure and does include 'https://' in the URL
- The link directs you to an unknown website unaffiliated with OU

Feedback for mindfulness training condition

- STOP and do not immediately click on the link.
- THINK about the email request.
    - Does the request ask for sensitive or private information? YES! This email asks for your private OU information
    - Is the email unexpected or rushed? YES! This email is rushed because you need to update your account immediately before it closes.
    - Does the request make sense? NO! This request does not make sense because you do not know what SunsetGates is.
- CHECK with a third-party source (OU Help Desk) before taking action.

From "University of Oklahoma" <donotreply@ou.edu>
To: donotreply@ou.edu
Subject: Be the First to Know
Date: Tue, 31 Jan 2017 18:36:31 +0730

Severe Weather Preparation
Severe weather can develop quickly and unexpectedly during this time of year. We want to make sure you are fully prepared to react and respond in such an event.

For more information on OU's emergency preparedness and procedures, please visit: https://www.ou.edu/emergencypreparedness/

OU Information Technology, OU Emergency Preparedness, and OUPD

Why is this a legitimate email?

Feedback for rule-based training condition

- The sender's email address is unknown and not from OU
- The link is not secure and does include 'https://' in the URL
- The link directs you to an unknown website unaffiliated with OU

Feedback for mindfulness training condition

- STOP and do not immediately click on the link.
- THINK about the email request.
    - Does the request ask for sensitive or private information? NO! This email does not ask for any private or sensitive information.
    - Is the email unexpected or rushed? NO! This email is not rushed because it is not forcing you to view the emergency preparation information.
    - Does the request make sense? YES! This request makes sense and comes from an OU-affiliated source.
- CHECK with a third-party source (OU Help Desk) before taking action.

Appendix F: Practice Test

From "OU IT" <ouit@gmail.com>
To: ouit@gmail.com
Subject: Upgrade Your Email Storage
Date: Tue, 10 Jan 2017 02:36:31 +0730

Dear OU Outlook Email User,

We noticed that your mailbox has exceeded the allocated storage limit as set by our administrator. You will not be able to send or receive email until you upgrade your allocated quota for effective use.

To upgrade your quota now, you need to click the link below to fill the upgrade form:

Click here

Failure to do this will make your account inactive.

University of Oklahoma Support Team
640 Parrington Oval, Norman, OK 73019 USA
Phone: (405)-325-2292

From "Microsoft Outlook Support Desk" <update@microsoftoutlook.com>
To: update@microsoftoutlook.com
Subject: Server Software Update Required
Date: Mon, 6 Mar 2017 09:30:31 +0730

We will be performing several software updates on our servers today at 9pm CST (2:00 GMT). The maintenance is required in order to keep our servers secure and up-to-date.

All users are required to upgrade his/her account automatically by clicking on the admin portal URL below to go to the email upgrade page.

Admin Access Portal

Our website, blog, and support forum may be momentarily unavailable around that time. We expect only a very short interruption of our form processing service (i.e., a few seconds while the web server software is resetting). For security reasons, the upgrade portal link will expire within 24 hours.

Microsoft Outlook Web App
IT Support

From: "OU Canvas" <canvas@ou.edu>
To: noreply@ou.edu
Subject: Canvas Access: Important Course Error Alert
Date: Thu, 16 Mar 2017 11:26:44 +0730

We detected something unusual about a recent sign-in to your Canvas account. For example, you might be signing in from a new location, device or app.

To keep you safe, we've blocked access to your inbox, contacts list and calendar for that sign-in. Please review your recent activity and we'll help you take correct action. To regain access, you'll need to confirm your identity.

Thanks,
Canvas Administrative.

From: "Netflix" <info@mailer.netflix.com>
To: noreply@netflix.com
Subject: Confirmation of changes to your membership
Date: Mon, 09 Jan 2017 10:11:15 +0730

NETFLIX

Your Price Change

The price for your Standard plan (2 screens at a time + HD) has changed to $9.99. This will take effect on your next billing date.

You can review your membership details at any time by visiting Your Account. As always, if you have questions, we are happy to help. Please visit the Help Center for more information.

- The Netflix Team

From: "Dropbox" <no-reply@dropboxmail.com>
To: noreply@dropboxmail.com
Subject: Resetting passwords from mid-2012 and earlier
Date: Tue, 9 May 2017 07:21:12 +0730

Hi,

We're reaching out to let you know that if you haven't updated your Dropbox password since mid-2012, you'll be prompted to update it the next time you sign in. This is purely a preventative measure, and we're sorry for the inconvenience.

To learn more about why we're taking this precaution, please visit this page on our Help Center. If you have any questions, feel free to contact us at password-reset-help@dropbox.com.

Thanks,
The Dropbox Team

From "University of Oklahoma" <donotreply@ou.edu>
To: donotreply@ou.edu
Subject: OU Alert Account Information
Date: Wed, 22 Feb 2017 02:36:31 +0730

TO: All Students, Faculty, and Staff

OU ALERTS!

Be the first to know - enter your text messaging number at accounts.ou.edu. When school is closed or there is an emergency on campus, we want you to be the first to know! Please visit your account and confirm your cell phone in the "Mobile Phone" field to make sure you receive campus notifications.

If you need help, please call the IT service desk at 325-HELP (4357).

Appendix G: Overlearning Test

From "OU IT Services" <ouit@ou.edu>
To: students@ou.edu
Subject: OU IT Systems Maintenance
Date: Wed, 10 May 2017 12:36:31 +0730

Hello OU Students,

There will be additional IT maintenance today between 8am – 5pm. During this time, some IT systems and applications may be affected, and you may experience brief outages.

Please upgrade your mailboxes (size to 20.0GB) by clicking IT SYSTEM AND MAINTENANCE.

Thanks,
OU Information Technology

From: "Dropbox" <no-reply@dropbox.com>
To: noreply@dropbox.com
Subject: Verify your email
Date: Fri, 07 Apr 2017 07:21:12 +0730

Hi,

Someone just shared a document with you via Dropbox. We just need to verify your email address before you can view/share the received file/folders. You are required to sign in with your email address to access your folder.

Verify your email

Thanks!
- The Dropbox Team

From "IT Services" <support@maildeliveryservice.net>
To: support@maildeliveryservice.net
Subject: Your Outlook Password Has Expired
Date: Tue, 28 Feb 2017 11:11:31 +0730

Dear Outlook User,

Due to recent suspicious activity, we have temporarily suspended your account. IT Security has implemented additional safeguards to help protect your account when there is a possibility that someone other than you tried to sign on. You may be getting this message because you signed in from a different location or device. If this is the case, your access may be restored when you return to your normal sign on method. As soon as possible, please log into your Outlook account from your normal computer. Click below to enter your information and reset your account.

Click to Reset your Account

Regards,
IT Security

From: "Information Technology" <ouit@ou.edu>
To: All Students (Norman) <student@ou.edu>
Subject: Your OU Student Email is Getting an Upgrade!
Date: Wed, 25 Jan 2017 15:22:33 +0730

Your OU Student Email is Getting an Upgrade!

Good news! Your OU student email is getting a FREE upgrade to Office 365. This new offering includes access to the latest Office 365 products, which are already available to you at portal.office.com (you can login now with your OU email address and password).

Need Help?
If you need assistance, please visit askit.ou.edu, call 325-HELP (4357) during normal business hours, or email needhelp@ou.edu at any time.

OU Information Technology

From "IT HelpDesk Norman" <needhelp@ou.edu>
To: students@ou.edu
Subject: D2L Maintenance
Date: Tue, 17 Jan 2017 11:16:32 +0730

Network Registration Reset

On Monday August 12th, Information Technology will conduct our annual Network Registration system reset in anticipation of the upcoming school year. This system is used to manage access to the OU network and educate students about the risks of peer-to-peer file sharing.

WHAT THIS MEANS TO YOU

Students will log in to the Network Registration system with their 4+4 and complete the copyright tutorial and quiz before registering their devices. You can find instructions on how to register a device here.

OU IT
innovate together
(405) 325-HELP
https://www.ou.edu/ouit

From: "IT HelpDesk Norman" <needhelp@ou.edu>
To: students@ou.edu
Subject: New Accounts Portal
Date: Fri, 20 Jan 2017 14:22:34 +0730

New Accounts Portal

Your account information is important for staying connected at the University of Oklahoma, and we want to make sure it's easy for you to manage and keep up to date. We're excited to share some of the great features on our new Accounts Management page that will help you:

- Recover Your Password
- Receive Emergency Text Messages
- Update Your Password
- Select an Email Alias

If you need assistance with any of these items, please call 325-HELP (4357).

OU Information Technology
it.ou.edu

Appendix H: Email Identification Test Version 1

From "OU IT Services" <ouit@ou.edu>
To: ouit@ou.edu
Subject: Account Update - Campus Wi-Fi
Date: Fri, 31 Mar 2017 11:22:31 +0730

Dear OU Student,

Information Technology has detected an error in your device's campus Wi-Fi connection. Any devices used to connect to campus Wi-Fi must be re-registered by clicking the link below.

DO NOT DELAY! Unregistered devices will not be permitted to access Wi-Fi.

To ensure continuous Wi-Fi on campus, click here to register your device now.

From "Password Reset" <password.reset@ou.edu>
To: password.reset@ou.edu
Subject: Password Reset Request
Date: Tue, 14 Feb 2017 12:36:31 +0730

Dear Student,

You have requested that your password be reset. Click the link below. You will be taken to the Account Management web page where you can change your password.

> Reset Password <

This link will expire in 24 hours and can only be used once.

Thank you,

The Account Team

From "OU Webmail Services" <donotreply@ou.edu>
To: donotreply@ou.edu
Subject: OU Account - Unknown Login
Date: Tue, 14 Mar 2017 06:36:31 +0730

Dear Account Owner,

Your e-mail account was logged in today by an unknown IP Address: 103.240.180.228. Kindly click here and login to validate and verify your e-mail account or your e-mail account will be automatically disabled from sending more messages.

We apologize for any inconvenience.

Sincerely,
University of Oklahoma Webmail Services

From "OU Bursar" <bursar@ou.edu>
To: donotreply@ou.edu
Subject: Mandatory Financial Aid Document
Date: Wed, 29 Mar 2017 19:36:31 +0730

Hi,

You have just received a mandatory financial aid document.

You are required to check this now by visiting bursar.ou.edu.

From: "Dropbox" <no-reply@dropbox.com>
To: noreply@dropbox.com
Subject: OU File Share
Date: Wed, 26 Apr 2017 07:21:12 +0730

OU shared with you an important document using Dropbox.

Click here to view

Sign in to access shared documents.

From: "Google Drive Team" <drive-noreply@google.com>
To: drive-noreply@google.com
Subject: Your 33 files stored in Google Docs are now in Google Drive
Date: Mon, 17 Apr 2017 12:53:41 +0730

Hi,
We're writing to let you know about important changes to Google Docs.

Google Drive is the new home for Google Docs

This means the 10 files that you own and the 23 files that have been shared with you will now be available in Drive, and you can access them anytime here.

You can still do everything you could before, like create, share, and collaborate with Google documents, spreadsheets, and presentations. Now, you can access your stuff anywhere, find files faster, and work with more web apps.

On behalf of files everywhere,
The Google Drive Team

From "eBay" <ebay@ebay.com>
To: donotreply@ebay.com
Subject: Help us protect your account
Date: Tue, 23 May 2017 09:16:41 +0730

Hi,

It's been more than a year since you last updated your personal info.

Keeping your personal info up to date can help better protect your account.

Sound like a good idea? All you have to do is go to eBay and take a look at your personal info to confirm that it's still correct. If you updated your personal info recently, please ignore this reminder.

Protect your account

Sincerely,
The eBay Accounts Team

From "OU - Office of the Bursar" <donotreply@ou.edu>
To: donotreply@ou.edu
Subject: Update 1098-T Address in oZONE
Date: Thu, 16 Feb 2017 02:36:31 +0730

Dear Student,

You are receiving this e-mail because our records indicate we will be providing you a 1098-T form for tax year 2015. These forms will be made available online to all students by January 31, 2016. Any student who does not specifically opt in to the Paperless 1098-T Program will also receive a paper copy of the 1098-T. Paper copies of this form will be mailed to the 1098-T Mailing Address on file with the University. In addition to providing you with a 1098-T, the University must also provide this form to the IRS with an accurate address. Please take a moment to verify that the University has an up-to-date 1098-T address for you. This address can be updated in oZONE by clicking on the "Update Addresses and Phones" link in the "Personal Information" channel, and then selecting the 1098-T Mailing Address from the list of available address types.

If you have any questions, please call the Office of the Bursar at (405) 325-3121.

Office of the Bursar
University of Oklahoma
1000 Asp Ave., Room 105
Norman, OK 73019-4071
Phone: (405) 325-3121
Fax: 325-6758

From "Learning System Administrator" <noreply@sumtotalsystems.com>
To: noreply@sumtotalsystems.com
Subject: University of Oklahoma OnPoint Required Training Enrollment
Date: Wed, 18 Jan 2017 10:32:31 +0730

Dear OU Student,

You have been assigned Sooner Fire Safety. To access and complete your training, go to onpoint.ou.edu and log in using your OUNet ID.

We strongly recommend completing this course on a device with a wired internet connection or stable wi-fi network.

This training course is assigned annually based on your last registration date. If you have recently completed this course, to avoid such a quick re-assignment in the future, make sure you stay in compliance with the 30-day training window. In the event of a fire, every minute counts. Knowing what to do or where to seek fire-fighting equipment or help can make the difference between life and death. OU provides fire extinguishers in all OU buildings to maximize safety for employees. The federal Occupational Safety and Health Administration (OSHA) requires that if an organization provides fire extinguishers for employees to use, the employees must be trained on how to properly use them.

Questions regarding the Fire Safety training, please contact the Fire Marshal's office at fire@ou.edu. For login questions, please contact your local IT service desk.

OnPoint LMS Administrator

From "OU IT" <ouit@ou.edu>
To: noreply@ou.edu
Subject: D2L Maintenance
Date: Wd, 11 Jan 2017 21:16:44 +0730

OU IT Scheduled Maintenance

OU IT has scheduled a Desire2Learn upgrade from 10:00 PM May 15th until 8:00 AM January 16th. During this maintenance window, D2L will be unavailable to all users on or off campus. It's important that you do not have any assignments (reading assignments, discussions, quizzes, or dropbox items) due during this time.

OU IT technicians will restore service as quickly as possible. Please check alerts.ou.edu for further updates. We apologize for any inconvenience and thank you for your patience.

If you need assistance, please call 325-HELP (4357) during normal business hours or email needhelp@ou.edu at any time.

OU Information Technology

Appendix I: Email Identification Test Version 2

From: "Netflix" <noreply@netl.com>
To: noreply@netflix.com
Subject: You need to update your payment method
Date: Mon, 22 May 2017 17:21:15 +0730

Update Payment Method

We were unable to bill your membership for the current month. To ensure that the service will not be interrupted, please update your payment method.

To update your payment method, click: Sign In to Netflix then you will be prompted to update your payment method.

- The Netflix Team

From "OU Information Technology" <ouit@ou.edu>
To: noreply@ouit.edu
Subject: Your OU email was logged in an unrecognized computer
Date: Wed, 5 Apr 2017 02:09:31 +0730

Unusual activity detected!

We detected something unusual about a recent activity on your account. To help keep you safe, we required an extra security challenge. You will need to update your email account below to confirm that the recent activity was yours and to regain access and enjoy our unlimited service.

Update Now

What happened?

- Using a shared computer to access your account.
- Logging in your Microsoft Outlook account from a blacklisted IP.
- Not logging off your account after usage.
- Thanks for using your Microsoft Outlook account to bring the people who matter most together in one place. You can change your connection settings anytime and find more ways to connect.

See you online,
OU Online Team

From "OU Admin" <MAILER-DAEMON@microsoftsql.net>
To: MAILER-DAEMON@microsoftsql.net
Subject: Re: Password Change
Date: Tue, 21 Feb 2017 09:16:42 +0730

Your message did not reach some or all of the recipients.

Subject: Password change!
Date: Friday, May 26, 2017 11:15am

The email system was unable to deliver the message, but not report a specific reason. Check the address and try again. If this still fails, contact your system administrator. #5.0.0 smtp; 5.1.0 - Unknown address error 550 5.1.1 unknown or illegal alias: (deliver attempts: 3).

Click here if you can't see the text

From "Human Resources" <hr@ou.edu>
To: noreply@ou.edu
Subject: Important Document
Date: Mon, 13 Mar 2017 02:36:31 +0730

Dear OU Student,

An important document has been sent to you by the Human Resources Department.

Click here to login to view the document now.

Thank you!
University of Oklahoma HR Department

From: "OU Canvas" <canvas@ou.edu>
To: noreply@ou.edu
Subject: Urgent Course Form
Date: Wed, 11 Jan 2017 11:26:44 +0730

Good morning,

An important course form has been posted to you on the Canvas Learning System.

Please sign in immediately to view the form.

Click here to sign in

Thank you,
Canvas Learning Notifications

From: "Amazon.com" <account-update@amazon.com>
To: noreply@amazon.com
Subject: Revision to Your Amazon Account
Date: Tue, 25 Apr 2017 12:22:22 +0730

Thanks for visiting Amazon! Per your request, we have successfully changed your password.

Visit your account to view your orders, make changes to any order that hasn't yet entered the shipping process, update your subscriptions, and much more.

Should you need to contact us for any reason, please know that we can give out order information only to the name and email address associated with your account. Thanks again for shopping with us.

From: "Desire2Learn Administrator" <learn@ou.edu>
To: noreply@ou.edu
Subject: You have been added to an OU D2L Course
Date: Mon, 16 Jan 2017 04:52:13 +0730

This is an automatic message sent because you have been added to CAS ONLINE ORIENTATION COURSE at the University of Oklahoma's learning management system, OU Desire2Learn (D2L).

If you are receiving this message, it is because someone has added you manually to a course or because you self-registered in a course inside OU D2L.

Click here to log in.

If you have problems logging in, please review the "Login Trouble?" area on the front page under the login box.

Students: This is not a confirmation of your official enrollment at the University. To verify your official enrollment, go to http://ozone.ou.edu.

D2L Administrator
learn@ou.edu

From: "Apple" <appleid@id.apple.com>
To: <do_not_reply@apple.com>
Subject: Your Apple ID password has been reset
Date: Fri, 27 Jan 2017 13:12:33 +0730

The password for your Apple ID has been successfully reset.

If you didn't make this change or if you believe an unauthorized person has accessed your account, go to iforgot.apple.com to reset your password immediately. Then sign in to My Apple ID to review and update your security settings.

If you need additional help, contact Apple Support.

Apple Support

From: "Hulu" <hulu@hulumail.com>
To: <hulu@hulumail.com>
Subject: Notice of Update to Hulu's Terms
Date: Wed, 8 Feb 2017 14:02:33 +0730

Hi,

We hope you're enjoying your summer. Here at Hulu, we are continually focused on improving our service and the viewer experience. To address some of the changes in our services, we've updated our Terms of Use. We want to ensure that we keep you informed about our practices, so we encourage you to review the full, updated version of our Terms of Use at https://www.hulu.com/terms.

Thank you for being a part of the Hulu community. If you have any questions, please feel free to reach out to us at legal@hulu.com.

Sincerely,
The Hulu Team

From "OU - Office of the Bursar" <bursar@ou.edu>
To: donotreply@ou.edu
Subject: OU Bursar Statement
Date: Tue, 10 Jan 2017 02:36:31 +0730

This is an automated message to inform you that a new billing statement has been issued and is now available for viewing at the website listed below. Remember, this site is available 24 hours a day to make paying your bill more convenient.

Use your username and password to log in to oZONE.ou.edu. Once logged in, click on the Money tab and select the View and pay account link. You can pay your bill, schedule a payment for a future date, or choose to have future bills paid automatically.

A 1.5% service charge with an APR of 18.00% will accrue on any balance remaining after the 21st of each month.

Office of the Bursar
University of Oklahoma
1000 Asp Ave., Room 105
Norman, OK 73019-4071
Phone: (405) 325-3121
Fax: 325-6758

Appendix J: Mock Phishing Test Version 1

From: "OU IT" <ouit@ou.edu>
To: noreply@ou.edu
Subject: OU Email Account Upgrade

Dear OU Staff/Student,

We apologize for any inconvenience caused due to a recent upgrade to the OU website and email service. Please log on to your account as soon as possible using your OU ID to be sure you have access to your email. This is to ensure that you don't miss out on important emails/contacts or lose valuable data.

Click here to log in

Sincerely,

IT Help Desk
University of Oklahoma

From "University of Oklahoma IT Department" <ouit@ou.edu>
To: noreply@ou.edu
Subject: Important Notice

Dear Account User,

Your email ID needs to be upgraded with our F-Secure R-HTK4S new version Anti-Spam/Anti-Virus/Anti-Spyware 2017. All users are required to verify their account using the link below.

https://www.ou.edu/softwareupdate

We are sorry for any inconvenience caused.

Sincerely,
University of Oklahoma
Web Admin Helpdesk

From "OU IT Department" <ouit@ou.edu>
To: donotreply@ou.edu
Subject: Urgent: OU Account Compromised

Hello,

Your OU account may have been recently compromised, and your account may be suspended in 48 hours. We just need you to review a few details for us, and we would get your account running without hassles again.

Please click below to review details.

Review Account

Sincerely,
OU IT Department

From "OU Admin" <donotreply@ou.edu>
To: donotreply@ou.edu
Subject: You Have (1) New Message

Dear Student,

You have unread messages from the OU Administrative Office. Please kindly click here and log in for you to read the messages.

Yours in service,
Admin Office
University of Oklahoma

From "HR Department" <hr.department@corp-hr.com>
To: hr.department@corp-hr.com
Subject: Updated Building Evacuation Plan

The University of Oklahoma is committed to providing the highest level of preparedness and emergency response for those working in or visiting our building(s). Being prepared starts with reviewing the evacuation plan.

In keeping with this commitment, we have updated our building evacuation plan. It is required that you sign in and acknowledge you have read the plan.

Appendix K: Mock Phishing Test Version 2

From: "OU IT" <ouit@ou.edu>
To: noreply@ou.edu
Subject: OU Outlook Account Information

Hi,

We received your request to delete your Outlook account permanently.

Please reconfirm your request to continue using our service.

If no action taken in less than one hour, your account will be permanently deleted on our database.

Have a great day!
©University of Oklahoma

From: "OU IT" <ouit@ou.edu>
To: students@ou.edu
Subject: OU Account Information

Hello,

This is to notify all students and staff members of the University of Oklahoma that we are validating active accounts.

Please kindly confirm that your account is still in use by clicking the validation link below:

Validate Email Account

Sincerely,

OU IT Help Desk
Office of Information Technology

From "OU Accounts" <donotreply@ou.edu>
To: donotreply@ou.edu
Subject: Review Your OU Information

We are contacting you to remind you that our Account Review Team identified some unusual activity to your OU Account.

We advise to verify your account to keep it activated.

https://www.ou.edu.

Thank you.

University of Oklahoma Service Team

From "David L. Boren" <noreply@ou.edu>
To: noreply@ou.edu
Subject: Important Announcement from David L. Boren

Good Morning OU Family,

Please click here for an important announcement from David L. Boren.

Thanks,

David L. Boren
President

From "University of Oklahoma" <noreply@ou.edu>
To: noreply@ou.edu
Subject: Urgent - Campus Construction Alert

Hello,

There is new construction being conducted on campus. We require everyone to read and follow the protocol.

Click here to view

Thanks,
University of Oklahoma