# Training to Mitigate the Threat of Phishing Attacks: A Mindfulness Approach

## Abstract

Despite significant investments in technology to combat phishing, firms lose billions of dollars each year due to phishing attacks. Anti-phishing training using behavioral modeling has reduced vulnerability to phishing attacks; however, there is some dispute regarding training’s proper level of conceptualization. Researchers and practitioners have embraced concrete training approaches that prescribe a search for specific cues or adherence to discrete rules to avoid phishing messages. We advocate for a more abstract training approach which is focused on the mental model individuals use to evaluate suspicious messages. The abstract approach, based on the concept of mindfulness, encourages individuals to move from mindless assessments to carefully scrutinizing the actions called for by emails. To evaluate these completing training approaches, we developed two anti-phishing training programs using behavioral modeling: an abstract mindfulness program and a concrete situation-specific training program. We tested their relative effectiveness in a field study at a US university that involved 355 email users, including students, faculty and staff. To evaluate the robustness of the training, we delivered each training program in one of two formats (text-only or graphics) and used generic and customized phishing messages. Results provide support for the abstract mindfulness approach as a more effective means of training individuals to avoid phishing attacks than the concrete situation-specific approach.

## Keywords: phishing, training, spear phishing, mindfulness, mindlessness

# Training to Mitigate the Threat of Phishing Attacks: A Mindfulness Approach

# Introduction

We all receive them: email messages that ask us to click on a link to avoid catastrophes such as saving our bank accounts from being closed or our email accounts from imminent deletion. Some emails are readily identified as fraudulent, others might require more consideration, but a few fool even the keenest evaluators ([Jackson et al. 2007](#_ENREF_31)). These kinds of threats against individuals are increasing. Symantec’s Internet Security Threat Report ([2014](#_ENREF_72)) stated that in 2013 there was a 91% increase in phishing campaigns. But not only does phishing threaten individuals, it also presents a substantial risk for organizations. Of all the phishing campaigns detected, 39% were sent to large enterprises (over 2500 employees). For example, between November 27th and December 15th in 2013, the credit and debit card information of more than 70 million people who bought goods at Target stores were stolen by cybercriminals who were able to gain access by using login information garnered during a phishing attack ([Bjorhus 2014](#_ENREF_7)). In another example in 2013, an Associated Press (AP) employee responded to a phishing attack which allowed the phishers to monitor the employee’s keystrokes and hack into AP’s official Twitter account. Using the Twitter account, the phishers posted that a bomb exploded at the Whitehouse, which caused the Standard & Poors Index to fall by $136 billion ([Dave 2013](#_ENREF_15)). Clearly, phishing is a significant problem to both consumers and large enterprises.

Phishing is a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve another’s confidential credentials, collect private information, or install malicious software on another’s machine by imitating electronic communications from a trustworthy source ([Hong 2012](#_ENREF_29); [Myers 2007](#_ENREF_57)). Phishing is typically carried out through email, although it has also been employed in text messaging and through social media ([Jagatic et al. 2007](#_ENREF_32)). A common phishing attack consists of an unsolicited email sent to an Internet user which requests personal or private information (e.g., login credentials, banking information). The email may appear to be from a legitimate source and it directs users to a fraudulent website which appears to represent a legitimate organization. If the user supplies the requested information, the phisher may then sell the information to other criminals or use the information to assume the user’s identity, commit financial fraud, or steal other private information. Monetary damages from phishing attacks have been estimated to total several billion dollars annually ([Gartner Group 2007](#_ENREF_20); [Hong 2012](#_ENREF_28)). But the potential damage to organizations spreads beyond financial losses to include theft of corporate secrets ([e.g., Markoff 2008](#_ENREF_52)), stealing classified information ([e.g., Hesseldahl 2011](#_ENREF_27)), and espionage ([e.g., Grow et al. 2008](#_ENREF_23)).

A typical phishing attack consists of blanketing a large number of email users with messages soliciting information. As information about individuals becomes publically available, phishers have increasingly turned from sending generic messages to sending customized messages to specific organizations, groups within an organization (e.g., executives), or even targeted individuals ([Federal Bureau of Investigation 2009](#_ENREF_18)). For example, using stolen user information, phishers assumed LinkedIn’s identity to attempt to elicit information from LinkedIn customers ([Perlroth 2012](#_ENREF_60)). Customized attacks are effective because they draw on existing pools of trust and knowledge to elicit information from potential victims. Such customized attacks, sometimes called spear phishing, have even resulted in serious security breaches. For example, an attachment in an email to a senior executive at the defense contractor Booz Allen Hamilton, ostensibly containing a request from the Pentagon, actually contained malware that stole sensitive information ([e.g., Grow et al. 2008](#_ENREF_23)).

To mitigate the danger posed by generic and customized phishing attacks, three primary techniques have been advanced: 1) automated prevention whereby phishing emails and websites are automatically discovered and quarantined or removed; 2) better warning mechanisms for when users encounter potential phishing attacks (e.g., within an Internet browser or email software); and 3) user training where users are taught to identify and avoid phishing emails and phishing websites ([Hong 2012](#_ENREF_29)). Although technical solutions (e.g., techniques 1 and 2) have been widely investigated ([see Kumaraguru et al. 2010](#_ENREF_42)) and have improved defenses against attacks ([Almomani et al. 2013](#_ENREF_2)), phishers continue to draw in victims each year. In part, this is because technical solutions lack the ability to detect each new permutation of phishing attacks ([Liu et al. 2006](#_ENREF_48)). In addition, Internet protocols (e.g., SMTP) and services (e.g., DNS) require substantial change if they are to be used to effectively identify phishing attempts ([Webber et al. 2012](#_ENREF_80)). Our focus on the user is important because, if technical solutions fail to detect phishing e-mails, it is ultimately the user who decides whether to respond to a phisher’s request for information. Even though users constitute the final defense against phishing e-mails, scant academic attention has been paid to the design of anti-phishing training programs ([Kumaraguru et al. 2010](#_ENREF_42)).

Past information systems (IS) research has demonstrated a clear benefit to behavior modeling as a general strategy for training individuals about IS topics ([Santhanam et al. in press](#_ENREF_63)). However, within behavior modeling, there are two variants of training approaches: one that is more concrete and prescribes discrete actions that are required from the learner; the second is more abstract and equips learners with mental structures that link training material with existing knowledge ([Sein et al. 1989](#_ENREF_67)). Both training approaches have produced success in the IS domain, but differences have emerged in their relative effectiveness according to the task and individual differences ([Bostrom et al. 1990](#_ENREF_9); [Santhanam et al. in press](#_ENREF_63)). Past anti-phishing research and practice has largely embraced the concrete training approach (e.g., [Cranor 2008](#_ENREF_14); [Kumaraguru et al. 2010](#_ENREF_42)). But there are several reasons (discussed below) why the conceptual training approach is beneficial and may even be superior to the concrete approach. Therefore, we focus this paper on the competing approaches to train users to evaluate suspect emails. Our primary research questions are:   
*RQ1: Does behavioral training reduce the likelihood that email users will respond to a phishing attack?   
RQ2: What is the most effective approach (conceptual or concrete) for conducting anti-phishing training?*

To address our research questions, we created two computer-based training programs based on competing theoretical approaches. The first uses a concrete approach to create situation-specific training and has been shown to be effective in past research (e.g., [Cranor 2008](#_ENREF_14); [Kumaraguru et al. 2010](#_ENREF_42)). The second uses a novel conceptual approach and is based on mindfulness and systematic information processing (Langer 1989). We tested these two training approaches in text-only and graphics-based formats in a field experiment at a Midwestern university where students, faculty, and staff participated in the training. Then, with the cooperation of university officials, we carried out generic and customized phishing attacks on the university students, faculty and staff, soliciting from them their university credentials. The results showed that the conceptual approach using mindfulness outperformed the concrete, situation-specific training approach in countering both generic and customized phishing messages, regardless of the presentation format employed in the training.

# Theoretical Development

Behavior modeling is a training strategy wherein desired behaviors are demonstrated and practiced by targeted learners. Behavior modeling typically: 1) describes the phenomenon, 2) provides cues or rules for identifying the phenomenon, 3) provides an opportunity to practice the behavior, and 4) provides reinforcement following the practice ([for example see Compeau et al. 1995a](#_ENREF_12)). Behavior modeling has been shown to be effective in both in-person and computer-based training environments. In a systematic review of training strategies, Santhanam and colleagues ([in press](#_ENREF_63)) found behavior modeling to be more effective than alternative training methods such as self-study ([Simon et al. 1996](#_ENREF_69)) and lecture-based instruction ([Bolt et al. 2001](#_ENREF_8); [Compeau et al. 1995a](#_ENREF_12); [Johnson et al. 2000](#_ENREF_37); [Simon et al. 1996](#_ENREF_69); [Yi et al. 2001](#_ENREF_86)). In short, behavior modeling is “one of the most widely used, well-researched, and highly regarded psychologically based training interventions” ([Taylor et al. 2005 p. 693](#_ENREF_73)).

Behavior modeling, which has roots in social cognitive theory ([Bandura 1986](#_ENREF_6)), is based on the notion that users will adopt behaviors they believe they can perform and behaviors they believe will have a valuable outcome. Behavior modeling satisfies both of these prerequisites for training new behavior ([Compeau et al. 1995a](#_ENREF_12)). When a user sees a demonstration of a desired behavior or decision model, the user will not only see how to accomplish the task, but will also learn what outcomes to expect. A rise in outcome expectations and self-efficacy, in turn, improve actual performance of the behavior because users will feel they know how to perform a valuable skill. While behavior modeling has shown repeated and robust effects in training individuals to adopt desired behaviors, there is some debate about level of conceptualization the behavior modeling should provide ([Gupta et al. 2010](#_ENREF_24); [Halasz et al. 1982](#_ENREF_26); [Sein et al. 1989](#_ENREF_67)).

On one hand behavior modeling is well-suited to demonstrate concrete anti-phishing actions that should be closely emulated in order to increase resistance to phishing attacks ([e.g., Kumaraguru et al. 2010](#_ENREF_42)). For example, one concrete action might include not opening any attachments from unknown senders and careful adherence to this rule should significantly reduce an individual’s susceptibility to phishing attacks. Behavior modeling of concrete actions transfers across similar tasks ([Mayer 1979](#_ENREF_53); [Mayer et al. 1972](#_ENREF_55)), therefore concrete anti-phishing actions designed to thwart a specific attack should be relevant to similar attacks but may be less relevant to novel attacks. On the other hand, behavior modeling is also well-suited to a more abstract explication of desired behaviors where individuals form or alter their mental models concerning desired actions (e.g., [Santhanam et al. 1994](#_ENREF_65); [Sein et al. 1989](#_ENREF_67)). For example, anti-phishing training could provide a general mental structure for allocating attention during the evaluation of emails. With more abstract behavior modeling, the training can focus on the mental representation of the evaluation, which then governs behavior. The abstract modeling approach has been shown to be relevant across a variety of tasks ([Mayer 1979](#_ENREF_53); [Mayer et al. 1972](#_ENREF_55)), but it is less explicit about desired behaviors.

## Hypotheses

### Concrete Behavior Modeling: Situation-Specific Training

In order for concrete phishing training to be relevant to the myriad contexts in which phishing occurs, researchers have developed training variants that teach users to identify cues in phishing emails or websites within a specific context (e.g., when accessing online financial information, confidential work documents, or personal information). We term this concrete training approach *situation-specific* because it prescribes specific courses of action (e.g., look for this visual or informational cue and follow this guideline) that decrease the likelihood of falling for a phishing attack within a specific context. Situation-specific training frames phishing prevention as an identification task and suggests that certain cues, if they are identified, or certain rules, if they are followed, will mitigate the risk posed by phishing. The situation specific training assumes that the rules are applied to a reasonably stable set of cues and that they serve as the basis for reliable heuristics that guide anti-phishing actions. As with other forms of concrete behavior modeling, learners using situation-specific training are introduced to the cues and rules, have a chance to practice identifying the cues or applying the rules, and through repetition and feedback acquire the experience and self-efficacy to apply the cues and rules effectively ([Kumaraguru et al. 2010](#_ENREF_42)).

The concrete approach is the predominate level of conceptualization in anti-phishing training and is employed across government, business, and community programs[[1]](#footnote-2) to train the general public about identifying phishing messages. Empirical testing of the approach has suggested it helps email users to identify phishing messages and avoid phishing attacks ([Cranor 2008](#_ENREF_14); [Kumaraguru et al. 2010](#_ENREF_42)). Hence, in a replication of previous research, we hypothesize that the concrete training approach will decrease the propensity of users to respond to phishing attacks.

*H1: The concrete training approach will decrease the likelihood that recipients will respond to phishing attacks*.

### Abstract Behavior Modeling: Mindfulness Training

Recent IS security research has suggested that individuals frequently process security risks using mindless information processing ([e.g., Vance et al. 2008](#_ENREF_76)), meaning that individuals rely on simple decision rules, mental short-cuts, or habit when processing security risks and rarely contemplate the ramifications of their actions ([see Kahneman 2011](#_ENREF_38)). This tendency is especially prevalent and problematic when email users encounter a phishing message ([Dhamija et al. 2006](#_ENREF_17); [Vishwanath et al. 2011](#_ENREF_78)). Mindless processing may result in email users not devoting sufficient attention to scrutinizing emails, leading them to miss cues that distinguish legitimate from phishing email, neglecting actions that may safeguard them from phishing attacks, and failing to consider the consequences of responding to a phishing email. Phishers appear to understand this tendency and compose phishing messages which take advantage of these decision rules (e.g., by using legitimate-looking logos and message designs) or encourage mindless processing (e.g., by inducing time pressure on the recipient to respond). Such tactics by phishers have been shown to be highly effective in soliciting responses ([Dhamija et al. 2006](#_ENREF_17); [Vishwanath et al. 2011](#_ENREF_78)). Conversely, research investigating the actions of email users who successfully identify phishing attacks revealed they avoid mindless processing, but rather scrutinized and verified emails that requested private information ([Wright et al. 2010a](#_ENREF_82)).

In light of these recent findings, we argue that individuals’ mental models could be altered using abstract behavioral modeling to increase the level of scrutiny suspicious emails receive. Specifically, we present an abstract approach based on the notion of mindfulness, which teaches individuals to carefully evaluate incoming email requests and the intentions of their senders rather than rely on mindlessly applied mental shortcuts. Instead of treating anti-phishing training as an identification exercise and focusing on knowledge of numerous cues and rules, we frame training as an exercise intended to elevate the degree to which individuals scrutinize emailed requests. This training approach encourages *mindfulness* to promote systematic information processing of phishing e-mails([Langer 1989](#_ENREF_43); [Langer 1997](#_ENREF_44)) and is intended to create new mental models concerning the allocation of attentional resources. Although some debate exists among researchers concerning the precise definition of mindfulness ([Brown et al. 2007](#_ENREF_10); [Lau et al. 2006](#_ENREF_46)), most researchers agree that mindfulness is more than mere attention and awareness of context and environment; it indicates a higher quality of consciousness characterized by receptive attention to current surroundings and experiences ([Brown et al. 2007](#_ENREF_10)). Mindfulness is conceptualized as possessing state and trait components ([Lau et al. 2006](#_ENREF_46)) and those who demonstrate higher levels of mindfulness also exhibit stronger behavioral control and self-regulation ([Brown et al. 2007](#_ENREF_10); [Leary et al. 2006](#_ENREF_47)). Promoting mindfulness through training has served as the foundation for clinical interventions for reducing stress ([Grossman et al. 2004](#_ENREF_22); [Shapiro et al. 1998](#_ENREF_68)), depression ([Teasdale et al. 2000](#_ENREF_74)) and other psychological problems ([Baer 2003](#_ENREF_4)).

This novel training approach equips individuals with mental tools that increase mindfulness when inspecting an email. First, in line with a mindfulness perspective ([Langer 1989](#_ENREF_43); [Langer 1997](#_ENREF_44)), individuals are explicitly encouraged to pause and reflect on their environment (i.e., an email and the context in which the email was received). A mindfulness approach promotes receptivity to surroundings, helps users to break out of cursorily evaluating emails, and encourages users to actively consider what each email asks of them. A concrete situation-specific approach, in contrast, encourages users to continuously scan emails for static cues and to always apply a standard set of rules to identify phishing. With mindfulness training, emails with unusual requests, such as asking for personal information, requesting user credentials, or including an unexpected attachment, should trigger more active assessment by the email user. This component of training, while relatively simple, may induce a greater amount of email-focused scrutiny.

Second, individuals are instructed to engage in a process of active questioning, where they are to consider several questions when evaluating actions requested in an email (e.g., click on a URL, download an attachment). A wide variety of cues may indicate an email is a phishing message; however, all phishing attacks require recipients to take some action that compromises their security and privacy. Posing questions that highlight the actions requested by phishing messages gives individuals guidance on how they can mindfully evaluate potentially harmful emails. During the process of active questioning, the user is encouraged to consider the email senders’ motivation, the email’s contents and the context in which the email was received. The evaluative focus on emailed requests is consistent with previous mindfulness interventions (i.e., for mood, problems relating to others, self consciousness, memory; [Mace 2007](#_ENREF_49); [Mace 2008](#_ENREF_50)) as the individual is able to concentrate on his or her own actions in response to requests rather than focusing on cues in the phishing email or website (which are controlled by the phisher).

Finally, a central component of mindfulness is forestalling judgment to avoid improperly jumping to conclusions ([Baer et al. 2004](#_ENREF_5)). When encountering deception in general, people are often suspicious of deceptive messages, but are hesitant to label the messages as deception for fear of the possibility that they could be legitimate ([Vrij 2006](#_ENREF_79)). This training encourages email users to attend to any suspicion they may feel about actions requested by incoming emails and to verify emails with trusted third parties (e.g., IT department) to ensure the requests are valid. This approach may reduce email users’ reluctance to address emails that seem suspicious or out of place but do not rise to the level of a blatant phishing attempt.

*H2: The abstract training approach will decrease the likelihood that recipients will respond to phishing attacks.*

The abstract approach offers several advantages over the concrete approach, which are summarized in Table 1. Both training approaches rely on behavioral modeling and offer similar first steps to describe the phenomenon as well as follow up steps of practicing and reinforcement; however, the provision of static rules and cues in situation-specific training may be ill-suited for phishing for three reasons. First, the concrete approach is only applicable when a phisher’s message contains recognizable cues or violates rules the recipient knows. In other words, in relying on situation-specific training, phishing recipients depend on phishers to make mistakes (e.g., using a poorly worded email message, suspicious email address, illegitimate website) in order for the training to be successful. Also, as recommendations and rules protecting email users against phishing become well known, successful phishers will seek to improve their tactics by designing messages that circumvent those rules. This risk is especially salient as information useful for phishing customization becomes more widespread. In a sense, phishers and security personnel are engaged in a game of cat and mouse: once security personnel identify and publicize a cue that enables users to recognize phishing, phishers may change their techniques to circumvent the rule. In contrast to a list of rules or cues, the abstract approach encourages close examination of any email that requests something protected, regardless of the potentially authentic nature of the email. By encouraging mindful evaluation of email, even when phishing emails become more sophisticated and customized, trainees will still take note of the actions requested by phishing emails and be less likely to respond.

Table 1 – Differences between Mindfulness and Situation-Specific Training Approaches

|  |  |  |
| --- | --- | --- |
| **Characteristic** | **Abstract** | **Concrete** |
| Scope | Holistic | Contextualized |
| Training Objective | Elevate scrutiny of incoming emails containing requests for action | Increase knowledge and use of numerous cues and rules to identify phishing messages |
| Theoretical Underpinning | Mental model that guides the allocation of attention | Behavioral model of cue recognition and rule implementation |
| Complexity of Training | Simple. Contains basic guidelines to determine which emails require more scrutiny | Complex. Contains numerous cues and rules to identity phishing messages |
| Applicability of Training | Applies to phishing attacks that contain requests for action | Applies to phishing attacks where the message contains recognizable cues or violates rules |
| Trainee Resistance to Phishing | Enables resistance to multiple types of phishing attacks through elevated scrutiny of requests for action | Enables resistance only when phishing cues are evident or when learned rules are violated. |

Second, there are many different types of phishing messages, and phishers try to take advantage of a variety of decision rules individuals use to evaluate emails ([Wright et al. Forthcoming](#_ENREF_84)). As a result, a wide range of potential cues may indicate that an email or website is illegitimate and part of a phishing attack. In order for situation-specific training to be thorough, it must provide instruction on the myriad cues and rules relevant to thwarting variants of phishing attacks. Essentially, such training must account for every possible situation. Consequently, the instructions may be too complex and may overload users with too much information about phishing cues. For example, the helpful recommendations listed by a non-profit anti-phishing group[[2]](#footnote-3) consume several pages of text. Training complexity may make evaluation more difficult as a user must recall and consider relevant cues and rules upon receipt of every new email. Training complexity may have even more damaging effects if users short circuit their evaluation by selectively applying only a few cues and rules or avoid evaluation all together. In contrast, the abstract mindfulness approach is simple and encourages careful evaluation of only a few critical items in any email. For example: Is the email asking for something unusual, such as personal information or credentials? These simple points of assessment can be used by email users without a deep understanding of phishing in its many varieties. Further, if any suspicion is raised, the user is prompted to verify the email with a trusted third party rather than shoulder the entire load for identifying phishing messages.

Third, the mindfulness training’s objective will likely be more diagnostic in separating phishing messages from legitimate messages. As discussed previously, all phishing messages encourage recipients to violate their own security and privacy. Therefore, a focus on the request in the phishing message will likely generalize across forms of phishing attacks to a greater degree than focusing on specific rules or cues which may or may not be applicable during a specific phishing attack. The concrete approach focuses on judging *characteristics* of the email, such as the sender’s email or the domain of linked websites. In contrast, the abstract approach highlights the *purpose* of the email. By focusing on the purpose of emails, users should more easily be able to identify emails that merit additional scrutiny and suspicion without having to carefully assess the cues of every email they receive.

*H3: The abstract training approach will be more effective than the concrete training approach in decreasing the likelihood that recipients will respond to phishing attacks.*

To provide a more robust test of the training approaches’ efficacy, we evaluated two types of delivery formats. MIS research has a rich tradition of studying the efficacy of computer-based presentation types ([e.g., Tractinsky et al. 1999](#_ENREF_75)). Research suggests that graphical presentation enhances overall information acquisition and decision making ([Jarvenpaa 1989](#_ENREF_33); [Jarvenpaa et al. 1988](#_ENREF_34); [Speier 2006](#_ENREF_70)). Better cognitive fit between a graphical representation and the task has been the explanation offered for the improvement in performance ([Dennis et al. 1998](#_ENREF_16); [Vessey et al. 1991](#_ENREF_77)). Cognitive fit theory suggests that as a task increases in complexity, a user will rely more on and retain more information that is presented graphically ([Speier 2006](#_ENREF_70)).

In addition to work building on cognitive fit, social learning theory ([Mayer 2001](#_ENREF_54)) also predicts that instruction utilizing a graphics-based presentation format will be more effective because learners are more motivated to learn and the content is more memorable. Recent research in security and phishing training that builds on social learning (e.g, [Kumaraguru et al. 2010](#_ENREF_42); [Srikwan et al. 2008](#_ENREF_71)) has produced promising results in support of using graphics over text-only computer-based training. Therefore, we sought to extend this finding across multiple training approaches (i.e., concrete and abstract) in a more stringent, experimental test.

*H4: Training presented in a graphics-based format will be more effective in decreasing the likelihood that participants will respond to phishing attacks than training presented in a text-based format.*

## Covariates

In investigating the effects of training approach and training format on the likelihood that an individual will respond to a phishing attack, it is important to consider several relevant control variables. First, in order to isolate the effect of the abstract training approach and gauge its effectiveness, we captured and controlled for how mindful participants are in general when responding to email. This *trait* *mindfulness* scale was developed in accordance with Langer’s conceptualization of mindfulness ([Langer 1989](#_ENREF_43); [Langer 1997](#_ENREF_44)), but was specifically oriented to email usage. Trait mindfulness is a second-order factor with subcomponents: 1. alertness to distinctions, 2. orientation in the present, 3. awareness of multiple perspectives, and 4. openness to novelty. Alertness to distinction is the degree to which an email user identifies differences between her email practices and others’ practices. Orientation to the present refers to how individuals understand the context surrounding email usage or the “big picture.” Awareness of multiple perspectives refers to the ability of an individual to scan an environment and identify many points of view about proper email usage. Openness to novelty refers to an email user’s willingness to explore new features across various situations. All of the components are listed in Appendix A.

In addition, we captured propensity to trust ([Pavlou et al. 2004](#_ENREF_59)), perceived Internet risk ([Jarvenpaa et al. 1999](#_ENREF_35); [Malhotra et al. 2004](#_ENREF_51)), and computer self-efficacy ([Compeau et al. 1995b](#_ENREF_13)) and self-reported expertise in identifying phishing messages as these variables have been examined in recent phishing research ([e.g., Wright et al. 2010b](#_ENREF_85)) and play an important role in training efficacy ([e.g., Yi et al. 2001](#_ENREF_86)). Finally, since there were several disparities (e.g., age, education level) between groups in the organization we sampled (a university) we controlled for student, staff, and faculty status.

# Method

## Overview

We conducted a field experiment at a university to test our hypotheses of how training can mitigate the risk posed by phishing messages. In cooperation with university IT professionals, the institutional review board (IRB), and the university administration, we randomly assigned participants to treatment conditions, invited participants to join in anti-phishing training, and then conducted a phishing attack during which participants were directed to visit a fictitious website and entered their university usernames and passwords.[[3]](#footnote-4) Data were gathered by two primary means: 1. an online survey administered following the training and 2. participants’ actions related to the phishing attack.

## Participants

Participants came from a university[[4]](#footnote-5) located in the United States. A total of 1048 participants were randomly assigned to experimental conditions and were invited to participate in a form of anti-phishing training. A total of 371 responded to the invitation to participate in the training; however, 16 of the participants did not complete the training and were excluded from analysis. This left 355 participants who completed the training to comprise the training sample (a 33.9% completion rate). The status of participants in each sample is reported in Table 2. In return for participating in the phishing training, participants were entered into a drawing for an iPad or one of 5 gift cards for $50.

Table 2 – Participants description

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Age** | | **Phishing Experiences** | | **Phishing Emails Per Week** | | **Status** | |
| <20 | 26% | Knew someone who fell for an attack. | 54% | None | 19% | Faculty | 24% |
| 21-29 | 29% | Never personally fallen for an attack. | 70% | 1-5 | 59% | Staff | 21% |
| 30-39 | 15% | Came close to falling for an attack. | 16% | 6-15 | 15% | Students | 56% |
| 40-49 | 13% | Personally fell for an attack. | 3% | > 16 | 7% |  |  |
| 50-59 | 12% | Unsure if personally fallen for an attack. | 11% |  | |  |  |
| >60 | 5% |  |  |  | |  |  |

## Stimulus Materials

### Training Approach

Participants who underwent training were welcomed to the training by a message from the university CIO, which stressed the importance of the training and thanked them for their participation. Next, participants were told that the university was experiencing an increase in phishing attacks and were shown information about the adverse consequences of responding to a phishing attack (e.g., endangering personal and institutional resources, compromising confidential information). Then, participants were exposed to one of the training programs that were designed to test the competing training approaches: a *concrete* approach that encourages email users to follow several best practice recommendations for secure email use and an *abstract* approach that encourages email users to mindfully pause and reflect about the validity of requests they receive through email. These training programs and how they reflect the competing theoretical approaches are discussed in more detail below. Following training, participants were asked to practice identifying phishing emails and were instructed to identify two legitimate and two phishing emails. Correct answers and explanations consistent with the training approach (concrete or abstract) were provided immediately after participants submitted their answers. Training concluded with participants completing a knowledge test based on the specific training program that provided correct answers and explanations after the test was complete.

The concrete training content was derived from anti-phishing recommendations found in academic, governmental, non-profit, and corporate sources. We first gathered recommendations for email users as set forth by previous anti-phishing researchers ([Kumaraguru et al. 2010](#_ENREF_42)). We then reconciled this list with resources provided by the U.S. Federal Trade Commission,[[5]](#footnote-6) the non-profit group antiphishing.org,[[6]](#footnote-7) and anti-phishing best practices suggested by an international bank.[[7]](#footnote-8) The combined list of recommendations from these sources was long and in some cases, was customized to specific types of interactions (e.g., online purchases or online banking). Across sources, we identified six consistent recommendations shown in Table 3. As a final check to determine the suitability of these recommendations for a university environment, we presented the recommendations to two independent IT security managers employed at two different universities. The security managers confirmed the recommendations to be highly relevant in a university environment and, if followed, would substantially reduce susceptibility to phishing attacks. Therefore, these six recommendations formed the content for the concrete anti-phishing training.

Table –Recommendations for avoiding phishing attacks using the concrete approach

|  |
| --- |
| **Recommendations** |
| 1. Never click on a link or open an attachment in an email from an unknown sender 2. Access a website by typing the web address yourself 3. Do not reply to emails asking for private information 4. Real organizations such as banks or employers will never ask for private information in an email 5. Be suspicious of a website that asks for private information 6. Look for cues such as HTTPS in the address bar or a lock icon in your browser to identify a fake website |

The abstract training was developed using guidance drawn from clinical mindfulness research ([Langer 1997](#_ENREF_44)) that focuses on enabling individuals to be aware of their actions and the potential consequences of their actions ([Langer et al. 1987](#_ENREF_45)). In translating these findings to anti-phishing training, we created content to encourage email users to pause and consider their responses to emailed requests. In past mindfulness research ([e.g., Brown et al. 2007](#_ENREF_10)), reflecting before taking action was shown to predict self-regulation. Therefore, our mindfulness training cautioned email users against quickly responding to email requests and encouraged them to stop, consider what emails ask them to do, and then take appropriate action. Consistent with the hypothesized reasoning for mindfulness training’s effectiveness, it was designed around three key tasks that are easy to remember and apply: 1. Stop! 2. Think… 3. Check.

The first step, Stop!, is intended to be a trigger for individuals to pause any time an email contains a request (e.g., download an attachment, click on a link). These requests come with some risk and the Stop! stage encourages individuals to pause to examine these risks and avoid automatic, or routinized replies when email requests are made. The second step, Think…, encourages the individuals to scrutinize actions they are asked to perform and consider the sender’s motivation and context for the request. The questions individuals were instructed to ask themselves while considering the legitimacy of an emailed request are shown in Table 4. These questions were designed to be short and easy to remember, but at the same time promote reflection and receptive attention concerning the emailed request. Finally, individuals were instructed to Check. If, during the process of evaluation, any suspicion was raised, individuals were instructed to check with a trusted third party. In the case of this training program, the local IT help desk was provided as a point of contact that would assist email users in distinguishing legitimate email requests from fraudulent ones. The contents and screen shots for both the situation-specific and mindfulness training approaches are presented in Appendix B.

Table – Recommendations for avoiding phishing attacks using the abstract approach

|  |
| --- |
| **Recommendations** |
| 1. Stop! 2. Think…    1. Does the request ask for private or proprietary information?    2. Is the request unexpected or rushed?    3. Does the request make sense?    4. Why would the sender need me to do this? |
| 1. Check. |

To determine if the participants felt the two training approaches were helpful and effective, we examined the results of the phishing identification practice and knowledge test, which was administered as part of the training. Upon completion of the training, we also asked the participants if the training helped them learn how to identify phishing messages.[[8]](#footnote-9) Participants using the concrete approach performed well on the phishing identification practice and knowledge test with average scores of 3.27 (SD = .70) and 3.36 (SD = .80), respectively. They reported that the training was very helpful (M=4.10; SD = .85). Likewise, participants using the abstract approach did well on the phishing identification practice and knowledge test with average scores of 3.18 (SD = .81) and 3.53 (SD = .82), respectively. They also reported the training was very helpful (M=4.18; SD = .76). Independent samples t-tests revealed no differences between the training approaches. These results suggest that subjects felt that the training approaches were equally successful and perceived them as valuable.

### Training Format

The method of training delivery was also manipulated such that some participants received training in a text-only format while others received training through a graphics-based format. With the graphics-based format, we attempted to replicate the successful approach taken by other phishing researchers (e.g., [Kumaraguru et al. 2009](#_ENREF_40); [Kumaraguru et al. 2010](#_ENREF_42)) and developed a four panel, comic-strip-like format with three characters (an email user, a mentor, and a phisher) demonstrating how phishing works and how one can avoid phishing attacks. The instructional portion where concrete or abstract training approaches were used was presented in the second panel. The text-only format contained the same content, but only the text was provided to the participants. The formats for the concrete and abstract training approaches are presented in the Appendix B.

### Phishing Email

In coordination with the university IT department, we created a legitimate employee email account for a fictitious person. We then spoofed the legitimate account when sending the phishing email, which is a common practice among actual phishers. We created the account for several reasons: first, we wanted to recreate as closely as possible an actual phishing attack and needed a legitimate email address to spoof. Second, we didn’t want to direct backlash for the phishing message at an actual university employee. Finally, we wanted control over the account to monitor correspondence (i.e., verification attempts) from university email users. A total of 19 individuals attempted to contact the fictitious employee to inquire about the phishing email and we did not respond to the inquiries. Four individuals made repeated inquiries.

Although email addresses were publically available through the online university directory, we received participants’ university email addresses from the university administration. Further, the IT department agreed not to block the phishing emails or the phishing website. We used customizable mass-emailing software to manage the email distribution and tracked the number of emails that were returned as undeliverable or that bounced because of participants’ email client settings. The mass emailing-software spoofed the email address of the fictitious employee and sent the phishing email to a randomly selected block of university students, staff, and faculty addresses every 10 minutes. It was not feasible to send all emails at once, because doing so would have caused the spam filter to catch the messages.

The content of the phishing message was in two conditions: 1. Generic, and 2. Customized. The generic email invited participants to log in to a fictitious web portal that supposedly supplied several services to individuals affiliated with the university and displayed an out of town contact number for the supposed sender. The customized email included the same invitation, but also listed the name of the university several times (sometimes in an abbreviation), the university mascot, displayed a local phone number, and was customized to each recipient based on their role at the university (e.g., student, staff, or faculty). These customizations are consistent with previous phishing experiments executed in higher education environments ([Wright et al. 2010a](#_ENREF_82); [Wright et al. 2010b](#_ENREF_85)). Both emails contained a URL to the phishing website in plain text and a URL that contained a tracking number (e.g., myUniversity.org?p1234) that allowed us to track visits to the phishing website in addition to logins. No attempt was made to conceal the URL because it was top level .org domain that contained the acronym for the university. The text of the generic and customized phishing messages is shown in .

### Phishing Website

Participants who clicked on links in the phishing emails or typed the phishing URL in their browsers were directed to a fictitious website (Figure 1) that was designed by the research team to mimic legitimate university websites. To preserve privacy, logos and text identifying the university have been redacted from the website. When participants typed their usernames and passwords and clicked the Login button, the password was immediately deleted and was not transmitted or stored by the website. Only usernames were transmitted and recorded by the website. After participants logged in to the fictitious website, they were informed that website content was still being populated and that they should log in at a later date to view the content.

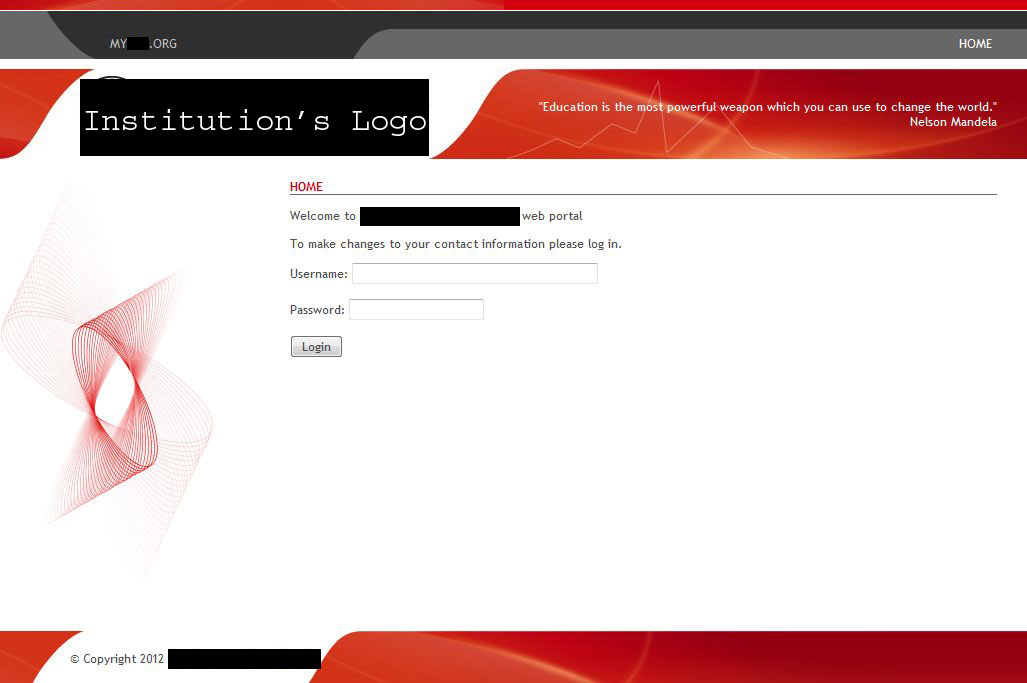


Figure – Fraudulent phishing website

**Table 5 – Generic and customized phishing emails**

|  |  |
| --- | --- |
| **Generic Phishing Email** | **Customized Phishing Email** |
| The university is planning a big upgrade to a new custom web portal. We value your input and invite you to test the new portal out. The new portal will allow you to:  • Access all university services online  • Purchase discounted software  • See what capital projects the university is working on  • Contact colleagues and friends in real-time  • And much more…  Please go to [Phishing Site] by 5pm on April 26th to register and login to your beta account. You can also access your account directly by going to [Phishing Site with Tracking Numbera]. You may have to copy and paste the URL into your web browser.  Sincerely,  [Fictitious Employee]  [Phishing Site] Administrator  [Phishing Site]  [Out of City Telephone Number] | Dear [University Name] Community Member,  As a [student, staff, faculty] community member, you are an essential part of the [University Name]. The university is planning a big upgrade to a new custom web portal. We value your input as a [student, staff member, faculty member] and invite you to test the new portal out. The new [University Name] portal will allow you to:  • Access all university services online  • Purchase discounted software  • See what capital projects the university is working on  • Contact colleagues and friends in real-time  • And much more…  Please go to [Phishing Site] by 5pm on April 26th to register and login to your beta account. You can also access your account directly by going to [Phishing Site with Tracking Numbera]. You may have to copy and paste the URL into your web browser.  Go [University Mascot]!  [Fictitious Employee]  [Phishing Site] Administrator  [Phishing Site]  [Local Telephone Number] |

aThe tracking number (e.g., myUniversity.org?p1234) allowed us to track visits to the phishing website in addition to logins.

## Procedure

Our experiment adhered to established guidelines for designing ethical phishing experiments ([Finn et al. 2008](#_ENREF_19)) (see Appendix C). We worked closely with the university administration (president’s office, legal counsel), IT department (chief information officer, support staff), and the IRB to minimize risk to the institution and participants and ensure relevant laws were followed.

Participants were randomly assigned to training conditions. Random assignment took place within roles so approximately equal groups of students, staff, and faculty were assigned to each condition. Before beginning the training, participants reported their level of expertise in identifying phishing email and were asked for their university username so they would be entered in a drawing for prizes. The participants then completed all sections of the training, then they completed a questionnaire capturing the other covariates (trait mindfulness, propensity to trust, propensity to take risks, computer self-efficacy). Finally, the participants recorded their attitudes about the effectiveness of the training.

To maintain proper experimental design, participants in one condition only filled out the covariate survey and did not actually receive the training. This design allowed us to isolate the effect of the training, independent of any priming effects resulting from the survey. The participants who only filled out the covariate survey were told that the IT department was interested in attitudes about phishing and that the survey would help them understand current attitudes about phishing. Table 6 presents the total number of participants in each condition for both the training and no training samples.

Table – Assignment of participants to experimental conditions

|  |  |  |  |
| --- | --- | --- | --- |
| **Conditions** | | **Generic Phishing Message** | **Custom Phishing Message** |
| Survey Only | | 33 | 40 |
| Concrete | Text | 34 | 40 |
| Graphics | 33 | 42 |
| Abstract | Text | 40 | 32 |
| Graphics | 27 | 34 |

Ten days following the training, participants were sent phishing emails. Prior to sending emails, we met with employees at the IT help desk to inform them of what we were doing and provide them with a script that they could use when responding to inquiries from email users. The script instructed email users not to respond to the suspicious email, to forward the email to the help desk employees, and to wait while the IT help desk investigated. We did this to mitigate the risk of users receiving actual phishing messages during the course of the experiment and to track the number of inquiries made by the participants. The help desk received 5 emails.

Participant usernames were collected for approximately four days before an astute staff member notified the entire campus via email of the phishing attack. This length of time for an active phishing attack is longer than the 62 hours that typical phishing attacks are active ([Moore et al. 2007](#_ENREF_56)) and is likely the result of the IT department’s cooperation. After the phishing attack was uncovered, we sent an email to all the participants disclosing our involvement, the purpose of the research, and protections that safeguarded their privacy. We also shared the training programs we developed with all university members. We received only one complaint from a staff member who, after the phishing attack was uncovered, needed to change passwords. Usernames collected during training were then matched with usernames collected by the phishing website by a researcher unaffiliated with the university where the phishing took place. The data were then anonymized and all links to participant identities were destroyed.

## Measurement

A measurement model was constructed to evaluate our scales’ reliability, convergent and discriminant validities. Consistent with the conceptualization of trait mindfulness as a second-order factor, we followed recommendations provided by Polites et al. ([2012](#_ENREF_62)) in generating the factor scores. We used the process outlined by Wright et al. ([2012](#_ENREF_83)) to construct a second-order confirmatory factor analysis using Mplus 6.1. A reliability analysis was then performed using Cronbach’s alpha and composite reliability scores ([Gefen et al. 2011](#_ENREF_21); [Werts et al. 1974](#_ENREF_81)). The Cronbach’s alpha scores were all above 0.72 which meet the recommendation that this score be above .70 ([Hair et al. 1998](#_ENREF_25)). Likewise, all composite reliability scores were also greater than the recommended .70 threshold ([Hair et al. 1998](#_ENREF_25)).[[9]](#footnote-10)

In the convergent validity tests, all factor loadings indicated compliance with the prescribed criteria of .70 ([Hair et al. 1998](#_ENREF_25); [Segars 1997](#_ENREF_66)). Convergent validity was further tested using the Average Variance Extracted (AVE) for each factor. Prior literature recommends that any factor should have an AVE above .50 ([Fornell et al. 1981](#_ENREF_20)) and AVE values for all of the factors were above this cutoff. AVE values were also used to assess discriminant validity, which allows for the evaluation of whether factors are statistically distinct from one another. The square-root AVE value for each factor was compared with the correlation with each of the other factors and consistent with previous recommendations, the square-root AVE was greater in every case ([Segars 1997](#_ENREF_66)). These results provide evidence of convergent and divergent validity (even among the first-order components of trait mindfulness). See Appendix A for a detailed summary of tests of the measurement model.

## Model Specification

Logistic regression was used to test the hypotheses. Logistic regression is intended for dichotomous dependent variables and permits categorical and continuous explanatory variables. The model for the training sample takes the following form:

Pr(Responding to Phishing Attack) = *β0*+ *β1*\*Student Status + *β2*\*Faculty Status + *β3*\*Trait Mindfulness + *β4*\*Propensity to Trust + *β5*\*Propensity to Take Risks + *β6*\*Computer Self Efficacy + *β7*\* Phishing Identification Expertise + *β8*\*Phishing Customization + *β9*\*Situation-Specific Training Approach + *β10*\*Mindfulness Training Approach + *β11*\*Graphical Training Format(2)

The participant status was recoded from a three-value categorical variable (i.e., student, staff, faculty) to two dichotomous dummy variables (student status, faculty status). This model also examines the effect of phishing email customization, training approach, and training format on the likelihood of responding to a phishing attack and is the central analysis of this research. Factor scores were calculated via a confirmatory factor analysis (CFA) using MPlus 6.1 and utilized in the model. This procedure provided participants’ mean-centered, composite score for each covariate.

# Results

Forty-seven participants in the training sample (including the survey-only condition) logged in to the fictitious website, resulting in a response rate of 13.2 percent. Descriptive statistics showing the number of participant responses and response rate in each condition are shown in Table 7. These findings are consistent with past industry reports on phishing response rates which indicate between a 10-15 percent rate of response for novice individuals ([Cisco Systems 2011](#_ENREF_11)). Figure 2 displays the timing of the responses to the phishing attack during the first four 24 hour periods after the first email was sent (10:00 AM). The attack generated the greatest response on the first day and decreased sharply on subsequent days. During the first 36 hours, responses were greatest in the evening when participants were most likely at home.

Table – Participant responses to phishing email

|  |  |  |  |
| --- | --- | --- | --- |
| **Conditions** | | **Generic Phishing Messagea** | **Custom Phishing Messagea** |
| Survey Only | | 8 (24.2%) | 9 (22.5%) |
| Concrete | Text | 4 (11.8%) | 6 (15.0%) |
| Graphics | 5 (15.2%) | 5 (11.9%) |
| Abstract | Text | 3 (7.5%) | 4 (12.5%) |
| Graphics | 2 (7.4%) | 1 (2.9%) |

a The number of responses is shown in absolute numbers and in percentages for each condition. Percentages are in parentheses



Figure – A) Responses to the phishing attack during first 4 24 hour periods; B) Responses to the phishing attack while attack by hours.

The sample size recommendation for logistic regression is that *P* + 1 be less than n0/10, where *P* is the number of explanatory variables in the model and n0 is the number of less frequent events (i.e., participants responding to the phishing email) ([Hosmer et al. 2000](#_ENREF_30)). However, due to the completion rate of those invited to participate in the training and the number of covariates considered, the size of training sample was less than the recommendation for full power. We chose to sacrifice power and include covariates for three reasons; first, including covariates at the expense of power is a conservative analysis approach ([Jo 2002](#_ENREF_36)). Second, theory mandates the presence of some covariates (e.g., trait mindfulness, computer self-efficacy) in the analysis. Finally, by including covariates, we rule out plausible alternative explanations for our findings. In Appendix D, we report the analysis without covariates. This analysis is consistent with sample size recommendations ([Hosmer et al. 2000](#_ENREF_30)) and the findings are unchanged.

Consistent with past MIS research ([e.g., Zmud et al. 2010](#_ENREF_87)), we evaluated competing models to assess model fit for the training and no training samples. Fit was evaluated using Akaike’s Information Criterion (AIC), which penalizes unnecessary model complexity ([Akaike 1973](#_ENREF_1)). A smaller value of the AIC indicates a better model fit. Table 8 provides the competing models for the training sample. The first model includes only the intercept and control variables (Model 1; Table 8) and the second contains the hypothesized model (Model 2; Table 8). The third model (Model 2; Table 8) contains a fully specified model complete with interactions. Based on the AIC, the hypothesized model (Model 2; Table 8) offers the best fit. In addition, all of the significant coefficients revealed in Model 2; Table 8 remain significant in Model 3; Table 8.

Consistent with recent research using logistic regression ([Hoetker 2007](#_ENREF_28)), we interpret significant findings by the magnitude of their marginal effects (also see [Kaufman 1996](#_ENREF_39); [Norton et al. 2004](#_ENREF_58)) rather than odds ratios. In a logistic regression model, explanatory variables do not have do not have a consistent, linear effect on the predicted outcome of the dependent variable; rather, the effect of an explanatory variable depends on the values of all the other explanatory variables in the logistic function ([Hoetker 2007](#_ENREF_28)). Therefore, to clearly see the effect of a significant explanatory variable, the marginal effect ([as shown by Petersen 1985](#_ENREF_61)) was calculated while holding the other explanatory variables constant.

Table – Test of Model Effects for Training Sample

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Model Factors | Model 1 (Controls Only) | | | Model 2 (Hypothesized) | | | Model 3 (Full) | | |
|  | B (SE) | Wald | Sig. | B (SE) | Wald | Sig. | B (SE) | Wald | Sig. |
| Intercept | -2.032 *(.403)* | 25.44 | <.001 | -1.133 *(.545)* | 4.33 | .037 | -.924 *(.655)* | 1.99 | .397 |
| Student Status | -.542 *(.451)* | 1.44 | .230 | -.121 *(.490)* | .06 | .806 | -.072 *(.492)* | .02 | .883 |
| Faculty Status | -1.247 *(.640)* | 3.80 | .051 | -1.45 *(.693)* | 4.41 | .036 | -1.441 *(.699)* | 4.25 | .039 |
| Trait Mindfulness | -4.665 *(.886)* | 27.73 | <.001 | -5.14 *(.959)* | 28.68 | <.001 | -5.232 *(.981)* | 28.44 | <.001 |
| Propensity to Trust | -.342 *(.233)* | 2.15 | .143 | -.305 (.*246*) | 1.53 | .216 | -.302 *(.250)* | 1.46 | .227 |
| Perceived Internet Risk | -.576 *(.258)* | 5.00 | .025 | -.670 (.*276*) | 5.89 | .015 | -.696 *(.282)* | 6.08 | .014 |
| Computer Self-Efficacy | .297 (.285) | 1.08 | .298 | .378 (.306) | 1.53 | .216 | .391 (.317) | 1.53 | .217 |
| Phishing Identification Expertise | -.131 *(.167)* | .613 | .434 | -.103 *(.170)* | .37 | .545 | -.086 *(.174)* | .245 | .621 |
| Phishing Customization |  |  |  | -.664 *(.393)* | 2.85 | .092 | -1.062 *(.747)* | 2.02 | .155 |
| Concrete Training Approach |  |  |  | -.419 *(.513)* | .67 | .415 | -.821 *(.847)* | .94 | .332 |
| Abstract Training Approach |  |  |  | -1.51 *(.568)* | 7.06 | .008 | -2.096 *(.880)* | 5.68 | .017 |
| Graphical Training Format |  |  |  | -.519 *(.464)* | 1.25 | .263 | -.379 *(.875)* | .19 | .665 |
| Phishing Customization \* Concrete Training Approach |  |  |  |  |  |  | .666 (1.097) | .37 | .544 |
| Phishing Customization \* Abstract Training Approach |  |  |  |  |  | 1.142 (1.166) | | .96 | .327 |
| Phishing Customization \* Graphical Training Format |  |  |  |  |  |  | -.251 (1.156) | .05 | .828 |
| Abstract Training Approach \* Graphical Training Formata |  |  |  |  |  |  | .674 (1.379) | .24 | .625 |
| Phishing Customization \* Abstract Training Approach \*  Graphical Training Formata |  |  |  |  |  | -1.562 *(2.016)* | | .60 | .438 |
| Model Summary |  |  |  |  |  |  |  |  |  |
| Omnibus Test of Model Coefficients | <.001 | | | <.001 | | | <.001 | | |
| -2 Log Likelihood | 205.29 | | | 191.76 | | | 190.01 | | |
| Cox and Snell R2 / Nagelkerke R2 | .184 / .339 | | | .215 / .396 | | | .219 / .403 | | |
| Hosmer and Lemeshow Test | .837 | | | .069 | | | .122 | | |
| Goodness of Fit Criteria |  |  |  |  |  |  |  |  |  |
| AIC | 219.29 | | | 213.76 | | | 224.01 | | |

a Since graphical training was crossed only with concrete and abstract training (see Table 6), the Concrete Training Approach \* Graphical Training Format and Phishing Customization \* Concrete Training Approach \* Graphical Training Format interactions are redundant and are not included in the fully specified model.

Although the effect from concrete training was in the hypothesized direction, the effect failed to reach significance. Thus, the results failed to support H1. Further, the format of the training did not exert a significant impact on participants’ likelihood to respond to phishing messages. This finding fails to support H4. However, the results concerning the abstract approach to training (H2 and H3) demonstrated significant results.

In support of H2, the abstract mindfulness approach to training significantly reduced the likelihood that people responded to the phishing attack. This effect persisted when controlling for trait mindfulness and other covariates. Participants who reported high mindfulness and high levels of perceptions of Internet risk were less likely to respond to the phishing attack. Also, members of faculty were less likely to respond to the phishing attack. To illustrate the impact of the abstract approach on training, we present the marginal effect of introducing mindfulness training on the probability that a participant will respond to a phishing email (Table 9). As significant covariates impact the marginal effect of the abstract training approach, we display the marginal effect at the mean value and plus or minus one standard deviation from the mean for trait mindfulness and propensity to take risks. We also display the marginal impact of the mindfulness training for faculty and non-faculty.

Table – Marginal effect of introducing abstract training

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Covariate Values** | **Conditions** | | **Probability of Responding** | **Marginal Effect of Abstract Traininga** |
| **Trait Mindfulnessb** | | | | |
| Low Mindfulness  (mean – 1 StDev = -.33) | Survey Only | | .444 | -.294 |
| Concrete | Text | .345 | -.240 |
| Graphics | .238 | -.174 |
| Abstract | Text | .150 |  |
| Graphics | .095 |  |
| Mean Mindfulness  (mean = .00) | Survey Only | | .128 | -.097 |
| Concrete | Text | .088 | -.067 |
| Graphics | .054 | -.042 |
| Abstract | Text | .031 |  |
| Graphics | .019 |  |
| High Mindfulness  (mean + 1 StDev = .33) | Survey Only | | .026 | -.020 |
| Concrete | Text | .017 | -.014 |
| Graphics | .010 | -.008 |
| Abstract | Text | .006 |  |
| Graphics | .004 |  |

Table 11 (continued) – Marginal effect of introducing abstract training

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Perceptions of Internet Risk****c** | | | | | | | |
| Low Internet Risk  (mean – 1 StDev = -.75) | Survey Only | | | .430 | | -.287 | |
| Concrete | Text | | .331 | | -.233 | |
| Graphics | | .228 | | -.167 | |
| Abstract | Text | | .143 | |  | |
| Graphics | | .090 | |  | |
| Mean Internet Risk  (mean = .00) | Survey Only | | | .313 | | -.222 | |
| Concrete | Text | | .231 | | -.169 | |
| Graphics | | .151 | | -.114 | |
| Abstract | Text | | .092 | |  | |
| Graphics | | .057 | |  | |
| High Internet Risk  (mean + 1 StDev = .75) | Survey Only | | | .216 | | -.159 | |
| Concrete | Text | | .154 | | -.115 | |
| Graphics | | .097 | | -.074 | |
| Abstract | Text | | .058 | |  | |
| Graphics | | .035 | |  | |
| **University Status****d** | | | | | | | |
| Faculty | Survey Only | | | | .107 | | -.081 |
| Concrete | | Text | | .073 | | -.056 |
| Graphics | | .045 | | -.035 |
| Abstract | | Text | | .026 | |  |
| Graphics | | .016 | |  |
| Staff | Survey Only | | | | .340 | | -.238 |
| Concrete | | Text | | .253 | | -.183 |
| Graphics | | .168 | | -.125 |
| Abstract | | Text | | .102 | |  |
| Graphics | | .063 | |  |
| Students | Survey Only | | | | .313 | | -.222 |
| Concrete | | Text | | .231 | | -.169 |
| Graphics | | .151 | | -.114 |
| Abstract | | Text | | .092 | |  |
| Graphics | | .057 | |  |
| a Marginal effects are shown in terms of probabilities  b In calculating the marginal impact of abstract training, phishing customization and a student population are assumed. Mean values for propensity to trust, perceived Internet risk, computer self-efficacy and phishing identification expertise are also assumed.  c In calculating the marginal impact of abstract training, phishing customization and a student population are assumed. Mean values for trait mindfulness, propensity to trust, computer self-efficacy and phishing identification expertise are also assumed.  d In calculating the marginal impact of abstract training, phishing customization is assumed. Mean values for trait mindfulness, propensity to trust, perceived Internet risk, computer self-efficacy and phishing identification expertise are also assumed. | | | | | | | |

To test H4, the hypothesized model (Model 2; Table 8) was tested again but participants who only completed the covariate survey were excluded from the analysis. This collapsed the training approach to a single variable with two values (concrete approach = 0 and abstract approach = 1) and permitted a direct comparison between the concrete and abstract approaches. A significant, negative coefficient would indicate that the abstract approach reduced phishing response above the effect from the situation-specific approach. As Table 12 illustrates, our finding supports H4.

Table – Test of model effects comparing abstract to concrete approaches

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Model Factors | Model 1 | | | |
|  | B (SE) | | Wald | Sig. |
| Intercept | -1.204 *(.555)* | | 4.70 | .030 |
| Student Status | -.442 *(.545)* | | .66 | .417 |
| Faculty Status | -2.321 *(1.124)* | | 4.27 | .039 |
| Trait Mindfulness | -3.497 *(.990)* | | 12.46 | <.001 |
| Propensity to Trust | -.215 *(.272)* | | .62 | .429 |
| Perception of Internet Risk | -.325 *(.308)* | | 1.31 | .253 |
| Computer Self-Efficacy | .356 (.345) | | 1.06 | .303 |
| Phishing Identification Expertise | -.238 *(.194)* | | 1.51 | .219 |
| Phishing Customization | -.400 *(.441)* | | .82 | .365 |
| Training Approach | -.978 *(.467)* | | 4.39 | .036 |
| Graphical Training Format | -.417 *(.446)* | | .88 | .349 |
| Model Summary |  | |  |  |
| Omnibus Test of Model Coefficients | <.001 | | | |
| -2 Log Likelihood | 149.05 | | | |
| Cox and Snell R2 | .139 | | | |
| Nagelkerke R2 | .282 | | | |
| Hosmer and Lemeshow Test | .871 | | | |
| Model Fit Criteria |  |  | |  |
| AIC | 207.77 | | | |

# Discussion

This research advances understanding of phishing and how people can be trained to resist phishing attacks. Our findings confirm past phishing research and advance them by introducing a novel abstract training approach. Specifically, we confirmed that training mitigated a phisher’s ability to elicit private information from e-mail users (see [Alnajim et al. 2009](#_ENREF_3); [Kumaraguru et al. 2007](#_ENREF_41); [Santhanam et al. 2008](#_ENREF_64)). We extended this body of work by demonstrating that a training approach’s theoretical underpinning and level of conceptualization affect its efficacy. Next, we outline the implications of our work for theory and practice.

## Implications for Theory

Critical to understanding the efficacy of training methods in general is an understanding each method’s theoretical foundations. We found that participants who completed training based on an abstract approach were significantly less likely to respond to customized and generic phishing attacks than participants who completed no training or those who completed training using a concrete approach. This finding has several theoretical implications for phishing research, security research, and training in general. First, consistent with past research ([e.g., Vance et al. 2008](#_ENREF_76)), our results support the notion that people respond to phishing attacks out of habit and cursory, heuristic processing of emailed requests. We show that a training approach directly focused on reducing the tendency to respond out of habit has a much greater effect on phishing mitigation than instructing email users in cues and rules that can be used to avoid phishing attacks. These findings elevate the alteration of mental models to govern mindless information processing as a critical step in anti-phishing and security training.

Next, in referent literatures, there has been debate about the efficacy of abstract mindfulness training and whether or not someone can be trained to be mindful ([Baer 2003](#_ENREF_4)). Our findings suggest that one can teach mindfulness techniques, and that individuals who receive such training go beyond mere awareness or problem identification to engaging in more secure behaviors. Both the concrete condition, which was based on the current state of the art (see [Alnajim et al. 2009](#_ENREF_3); [Kumaraguru et al. 2009](#_ENREF_40); [Kumaraguru et al. 2007](#_ENREF_41); [Santhanam et al. 2008](#_ENREF_64)), and the survey-only condition induced awareness of phishing in the participants. Yet, participants who completed training based on mindfulness were less likely to respond to a phishing attack than participants in the other conditions. This finding suggests that, as we hypothesized, the abstract mindfulness approach altered how participants responded to incoming email and improved the quality of attention. Thus, not only can mindfulness be taught, but it can be taught via computer-based training. This finding opens the door to additional research that examines how to increase mindfulness through computer-based training (e.g., clinical psychological interventions).

Our findings illuminate a paradox for phishing training research that while trainees felt equipped to protect themselves; in fact, their behavior suggested that they were not. We note that participants in the survey-only and concrete training conditions believed that they were well-equipped to counter phishing attacks. They reported that they knew what a phishing message looked like (M = 3.55; SD = 1.30) and were confident in their ability to detect them (M = 3.54; SD = 1.28).[[10]](#footnote-11) Had participants followed the guidance provided in the concrete training (e.g., Never click on a link or open an attachment in an email from an unknown sender; Be suspicious of a website that asks for private information), they would have avoided both the customized and generic phishing attacks. Nevertheless, many participants in the concrete training condition responded to the phishing attack. These findings highlight a distinct danger facing anti-phishing efforts: individuals may think they know how to respond to a phishing message, but not all of them do and whole organizations could be imperiled as a result. Participants in the abstract condition also reported a high level of expertise (M = 3.52; SD = 1.31) and confidence (M = 3.47; SD = 1.29) in identifying phishing messages. Yet in contrast to the results from the concrete and survey-only training conditions, participants in the abstract training condition showed lower susceptibility to phishing attacks. This finding suggests that the abstract approach may provide the additional benefit of reaching email users who already think they are capable of identifying phishing messages, but may not be.

Our work offers a theoretical framework upon which future researchers can build to elevate mindfulness in order to combat phishing or other information security threats. As we hypothesized, mindfulness can be increased in others by encouraging them to 1. pause; 2. observe the environment (perhaps with the direction of questions intended to promote deeper consideration of the environment); 3. focus on actions being requested; 4. forestall judgment if suspicion is raised and take action to verify the suspicion. These actions, when applied to the phishing context, elevated the participants’ quality of attention and reduced the response rate to the phishing attack. This framework for elevating mindfulness may also be effective in reducing the risk of other forms of social engineering that defy a completely automated solution and may improve adherence to seemingly prosaic company security policies. Additionally, training programs that suffer from similar difficulties as concrete phishing training (i.e. participants thinking their expertise is high, when, in fact, it is not) may benefit from an abstract mindfulness approach. If the ultimate goal of training is to shape habitual behavior (e.g., [Compeau et al. 1995a](#_ENREF_12); [Simon et al. 1996](#_ENREF_69); [Taylor et al. 2005](#_ENREF_73)), an abstract mindfulness approach to training provides a new area that merits additional attention.

Our findings suggest that content, not format, contributes to anti-phishing training’s effectiveness. In addition to comparing two training paradigms, we evaluated whether their effectiveness varied with training format. The content for each training approach (concrete and abstract) was presented in two different formats: text-only and graphics-based. Building on concepts drawn from social learning theory ([Mayer 2001](#_ENREF_54)) and cognitive fit ([Speier 2006](#_ENREF_70)), we hypothesized that a graphics-based training format would be more memorable and more effective in teaching users how to recognize and respond to phishing. We found that training via a text-only or graphics-based format were equally effective. Our finding is inconsistent with existing phishing research (e.g, [Kumaraguru et al. 2010](#_ENREF_42); [Srikwan et al. 2008](#_ENREF_71)) which showed better resistance to phishing attacks when training was presented graphically. Our findings imply that cognitive fit is roughly equivalent and the content was equally memorable between the text-only and graphics-based formats. Additionally, our finding implies that other facets of training (e.g., whether the training is based on a concrete or abstract approach) are much more important to training success than presentation format.

Finally, our findings illuminate the nomological network that shapes responses to phishing. Our analysis of covariates suggests that a population can segmented to identify those individuals who are most likely to respond to a phishing attack. Not surprisingly, participants who were low in trait mindfulness were highly susceptible to the phishing attack. Next, status at the university significantly influenced the probability that an individual would respond to a phishing message. These findings are consistent with past research which indicated age or education assists individuals in appropriately responding to phishing ([Hong 2012](#_ENREF_29)). Finally and also not surprisingly, individuals who perceived a low level of risk from performing tasks on the Internet were more likely to fall for phishing attacks. Fortunately, our findings also suggest that training using an abstract approach dramatically reduces the susceptibility of these vulnerable groups. For example, as shown in Table 11, for untrained students who exhibit low trait mindfulness, training can reduce the probability of responding to a phishing attack by 29.4 percent.

## Implications for Practice

Our results have several implications for practice. First, this study reinforces the importance of training users on how to respond to suspected phishing attacks. Email users’ ability to identify and avoid phishing attacks is an important, and perhaps critical, line of defense against phishing. However, while our results suggest that abstract mindfulness training may result in fewer security breaches, managers should be realistic with their expectations about phishing training. Even a mindfulness approach to training, as our results demonstrate, does not drive phishing response rates down to zero. Therefore, training is best positioned as part of a layered set of defenses that includes both technology-based (e.g., phishing site removals, automated warnings, filtering, and so on) and training components.

Second, results show that the theoretical approach that underpins a training program is crucial. The more effective training approach encouraged an active, mindful consideration of email messages. Further, individuals will not all benefit to the same degree from training using the abstract approach. Individuals who are young and inexperienced, low in trait mindfulness, low in perceptions of Internet risk will benefit disproportionally from the training while those who are older and more experienced, high in trait mindfulness, and high in perceptions of Internet risk will not derive as much benefit. Therefore, when allocating training resources, those charged with managing organizational security should consider not only the approach to training, but also the demographics of their employee population, when seeking to maximize the overall security of the organization.

Third, in this experiment, we delivered the training through relatively brief, online training sessions. Therefore, managers could potentially create and distribute anti-phishing training electronically to a large number of users. Our results imply that the presentation of the training need not be complex or costly. Results show that training consisting of only text was just as effective as training shown via a graphics-based presentation method. Additionally, given that the content for abstract mindfulness training is relatively simple, it could easily be adapted for other presentation methods, such as in a classroom or via video. What is important, as security specialists develop training programs, is that they direct attention to sets of behaviors that place organizations at risk (e.g., poor information processing practices), rather than complicated, ever changing, sets of cues that indicate an e-mail is from a phisher.

Fourth, the mindfulness approach we have applied offers significant benefits to users of anti-phishing training. We offer detailed explanations and illustration of our training materials in Appendix B and invite researchers and practitioners to use, modify, and expand these training materials to improve phishing mitigation efforts.

**Limitations and Future Research**

There are several limitations of this research, which provide opportunities for future research. First, the analysis is underpowered due to the high number of covariates included in the analysis and the small number of people who completed the training and responded to the phishing message. When tested without covariates, the significant findings did not change (see Appendix D); however, readers should interpret the non-significant findings with caution. Additionally, we acknowledge that our sample is vulnerable to selection bias because participants were recruited through email. While demonstrating effectiveness of training for individuals who respond to email solicitations is a valuable improvement, the participants may not reflect the practices of the general population. Hence, as is common for research on training, our study needs replication in diverse contexts.

Second, future research should investigate other training formats that may further increase the effectiveness of abstract training. We were able to successfully train users to be more mindful in how they deal with email through a simple, online format. Future work should consider how an interactive training format, such as an in-person training session, interactive software or creating teachable moments ([see Cranor 2008](#_ENREF_14)), might enhance user learning. Additionally, future research may investigate how a concrete approach might be integrated with an abstract approach. In certain training contexts (e.g., financial services), training may be required to explicitly cover certain topics in a situation-specific manner. Therefore, some merging of a concrete approach and mindfulness approach may be necessary. Understanding how a concrete approach can work in tandem with an abstract approach may yield further training gains.

Finally, an abstract mindfulness approach to training may be helpful in many other contexts aside from phishing. Since mindfulness encourages active awareness of context and surroundings, mindfulness training could easily be adapted to encourage appropriate behavior in other security settings. Furthermore, mindfulness training could be used to encourage better decision making in a variety of settings, such as employee behavior in social media. Employees could be trained to stop, and think about whether their behavior in a ‘public’ setting, like Twitter, Facebook or even company forums, could be construed as inappropriate. With this paper we have laid out the approach we have taken and hope that this approach may be useful to other researchers who wish to explore contexts other than phishing.

# Conclusion

Due to the limitations of technical anti-phishing techniques, this study introduced an abstract mindfulness anti-phishing training approach as an additional layer of defense against phishing attacks. Through a rigorous field test that compared the effectiveness of abstract and concrete approaches, we found that when individuals were taught to stop, think, and check the legitimacy of an email, they were far less likely to disclose private information than when exposed to concrete training. It is our hope that by improving the approach and contents of training, phishing will become less of a threat to the security of individuals and organizations.

# References

Akaike, H. 1973. "Information theory and an extension of the maximum likelihood principle," in *Proceedings of the Second International Symposium on Information Theory,* B. N. Petrov and F. Csaki (eds.), Akademiai Kiado: Budapest, pp. 267–281.

Almomani, A., Gupta, B., Atawneh, S., Meulenberg, A., and Almomani, E. 2013. "A Survey of Phishing Email Filtering Techniques," *IEEE Communications Surveys & Tutorials* (15:4), pp 2070-2090.

Alnajim, A., and Munro, M. Year. "An Anti-Phishing Approach that Uses Training Intervention for Phishing Websites Detection," Information Technology: New Generations, 2009. ITNG '09. Sixth International Conference on2009, pp. 405-410.

Baer, R. A. 2003. "Mindfulness Training as a Clinical Intervention: A Conceptual and Empirical Review," *Clinical Psychology: Science and Practice* (10:2), pp 125-143.

Baer, R. A., Smith, G. T., and Allen, K. B. 2004. "Assessment of mindfulness by self-report: The Kentucky Inventory of Mindfulness Skills," *Assessment* (11:3), pp 191-206.

Bandura, A. 1986. *Social Foundations of Thought and Action*, (Prentice Hall: Englewood Cliffs, NJ.

Bjorhus, J. 2014. "Target breach started as an e-mail phishing expedition.," StarTribune.

Bolt, M. A., Killough, L. N., and Koh, H. C. 2001. "Testing the interaction effects of task complexity in computer training using the social cognitive model," *Decision Sciences* (32:1), pp 1-20.

Bostrom, R. P., Olfman, L., and Sein, M. K. 1990. "The importance of learning style in end-user training," *MIS Quarterly* (14:1).

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

Cisco Systems 2011. "Email attacks: This time it's personal," <http://www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10339/ps10354/targeted_attacks.pdf:> San Jose, CA.

Compeau, D. R., and Higgins, C. A. 1995a. "Application of social cognitive theory to training for computer skills," *Information Systems Research* (6:2), pp 118-143.

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

Cranor, L. F. 2008. "Can Phishing Be Foiled?," *Scientific American* (299:6), pp 104-110.

Dave, P. 2013. "Email 'phishing' attacks by hackers growing in number, intensity.," LA Times.

Dennis, A. R., and Carte, T. A. 1998. "Using Geographical Information Systems for Decision Making: Extending Cognitive Fit Theory to Map-Based Presentations," *Information Systems Research* (9:2), pp 194-203.

Dhamija, R., Tygar, J. D., and Hearst, M. Year. "Why phishing works," Proceedings of the SIGCHI Conference on Human Factors in Computing Systems ACM, Montreal, Quebec, 2006, pp. 581-590.

Federal Bureau of Investigation 2009. "Spear phishers: Angling to steal your financial info."

Finn, P., and Jakobsson, M. 2008. "Designing and conducting phishing experiments," *IEEE Technology and Society* (6:2), pp 66-68.

Fornell, C., and Larcker, D. F. 1981. "Evaluating Structural Equations Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1), pp 39-50.

Gefen, D., Straub, D. W., and Rigdon, E. E. 2011. "An Update and Extension to SEM Guidelines for Admnistrative and Social Science Research," *MIS Quarterly* (35:2), pp iii-xiv.

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

Grow, B., Epstein, K., and Tschang, C. 2008. "The New E-spionage Threat," <http://www.businessweek.com/stories/2008-04-09/the-new-e-spionage-threat>.

Gupta, S., Bostrom, R. P., and Huber, M. 2010. "End-user training methods: what we know, need to know," *ACM SIGMIS Database* (41:4), pp 9-39.

Hair, J. F., Jr. , Anderson, R. E., Tatham, R. L., and Black, W. C. 1998. *Multivariate Data Analysis with Readings*, (5th ed.) Prentice Hall: Englewood Cliffs, NJ.

Halasz, F., and Moran, T. P. Year. "Analogy considered harmful," Proceedings of the 1982 conference on Human factors in computing systems, ACM, New York, NY, 1982, pp. 383-386.

Hesseldahl, A. 2011. "Lockheed Martin confirms it came under attack," <http://news.cnet.com/8301-1009_3-20067190-83.html>.

Hoetker, G. 2007. "The use of logit and probit models in strategic management research: Critical issues," *Strategic Management Journal* (28:4), pp 331-343.

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

Hosmer, D. W., and Lemeshow, S. 2000. *Applied logistic regression*, (Wiley: New York, NY.

Jackson, C., Simon, D., Tan, D., and Barth, A. 2007. "An evaluation of extended validation and picture-in-picture phishing attacks," in *Financial Cryptography and Data Security,* S. Dietrich and R. Dhamija (eds.), Springer Berlin / Heidelberg, pp. 281-293.

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

Jarvenpaa, S. L. 1989. "The Effect of Task Demands and Graphical Format on Information Processing Strategies," *Management Science* (35:3), pp 285-303.

Jarvenpaa, S. L., and Dickson, G. W. 1988. "Graphics and Managerial Decision Making: Research Based Guidlines," *Communications of the ACM* (31:6), pp 764-774.

Jarvenpaa, S. L., Tractinsky, N., and Saarinen, L. 1999. "Consumer trust in an internet store: A cross-cultural validation," *Journal of Computer‐Mediated Communication* (5:2).

Jo, B. 2002. "Statistical power in randomized intervention studies with noncompliance," *Psychological Methods* (7:2), pp 178-193.

Johnson, R. D., and Marakas, G. M. 2000. "Research report: the role of behavioral modeling in computer skills acquisition: Toward refinement of the model," *Information Systems Research* (11:4), pp 402-417.

Kahneman, D. 2011. *Thinking, fast and slow*, (Farrar, Straus and Giroux: New York, NY.

Kaufman, R. L. 1996. "Comparing the effects of dichotomous logistic regression: A variety of standardized coefficients," *Social Science Quarterly* (77:1), pp 90-109.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., and Pham, T. Year. "School of phish: A real-world evaluation of anti-phishing training," SOUPS '09 Proceedings of the 5th Symposium on Usable Privacy and Security, ACM, Mountain View, CA, 2009, p. 3.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L., Hong, J., and Nunge, E. Year. "Protecting People from Phishing: The Design and Evalaution of an Embedded Training Email Systems," Computer Human Interaction (CHI), ACM Press, San Jose, CA, 2007.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., and Hong, J. 2010. "Teaching johnny not to fall for phish," *ACM Transactions on Internet Technology (TOIT)* (10:2), p 7.

Langer, E. J. 1989. *Mindfulness*, (Addison-Wesley: Reading, MA.

Langer, E. J. 1997. *The power of mindful learning*, (Addison-Wesley Reading, MA.

Langer, E. J., and Piper, A. 1987. "The Prevention of Mindlessness," *Journal of Personality and Social Psychology* (53), pp 280-287.

Lau, M. A., Bishop, S. R., Segal, Z. V., Buis, T., Anderson, N. D., Carlson, L., Shapiro, S., Carmody, J., Abbey, S., and Devins, G. 2006. "The Toronto Mindfulness Scale: Development and validation," *Journal of Clinical Psychology* (62:12), pp 1445-1467.

Leary, M. R., Adams, C. E., and Tate, E. B. 2006. "Hypo-egoic self-regulation: Exercising self-control by diminishing the influence of the self," *Journal of Personality* (74:6), pp 1803-1831.

Liu, W., Deng, X., Huang, G., and Fu, A. Y. 2006. "An antiphishing strategy based on visual similarity assessment," *IEEE Internet Computing* (10:2), pp 58-65.

Mace, C. 2007. "Mindfulness in psychotherapy: an introduction," *Advances in Psychiatric Treatment* (13:2) March 1, 2007, pp 147-154.

Mace, C. 2008. "Mindfulness and the future of psychotherapy," *European Psychotherapy* (8:1), pp 129-139.

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

Markoff, J. 2008. "Larger prey are targets of phishing," in *New York Times*, <http://www.nytimes.com/2008/04/16/technology/16whale.html:> New York, NY.

Mayer, R. E. 1979. "Can advance organizers influence meaningful learning?," *Review of educational research* (49:2), pp 371-383.

Mayer, R. E. 2001. *Multimedia Learning*, (Cambridge University Press: Cambridge.

Mayer, R. E., and Greeno, J. G. 1972. "Structural differences between outcomes produced by different instructional methods," *Journal of educational psychology* (63:2), p 165.

Moore, T., and Clayton, R. Year. "Examining the impact of website take-down on phishing," Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit, ACM2007, pp. 1-13.

Myers, S. 2007. "Introduction to phishing," in *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft,* M. Jakobsson and S. Myers (eds.), Wiley: Hoboken, NJ, pp. 1-29.

Norton, E. C., Wang, H., and Ai, C. 2004. "Computing interaction effects and standard errors in logit and probit models," *The Stata Journal* (4:2), pp 154-167.

Pavlou, P. A., and Gefen, D. 2004. "Building effective online marketplaces with institution-based trust," *Information Systems Research* (15:1), pp 37-59.

Perlroth, N. 2012. "That was fast: Criminals exploit linkedIn breach for phishing attacks."

Petersen, T. 1985. "A comment on presenting results from logit and probit models," *American Sociological Review* (50:1), pp 130-131.

Polites, G., Roberts, N., and Thatcher, J. 2012. "Conceptualizing Models Using Multidimensional Constructs: A Conceptual Review and Guidelines for their Use," *European Journal of Information Systems* (21:1), pp 22-48.

Santhanam, R., Mun, Y., Sasidharan, S., and Park, S. in press. "Toward an integrative understanding of information technology training research across information systems and human computer interaction: A comprehensive review," *AIS Transaction on Human-Computer Interaction*).

Santhanam, R., Sasidharan, S., and Webster, J. 2008. "Using self-regulatory learning to enhance e-learning-based information technology training," *Information Systems Research* (19:1), pp 26-47.

Santhanam, R., and Sein, M. K. 1994. "Improving end-user proficiency: Effects of conceptual training and nature of interaction," *Information Systems Research* (5:4), pp 378-399.

Segars, A. 1997. "Assessing the Unidimensionality of Measurement: A Paradigm and Illustration Within the Context of Information Systems Research," *Omega* (25:1), pp 107-121.

Sein, M. K., and Bostrom, R. P. 1989. "Individual differences and conceptual models in training novice users," *Human-Computer Interaction* (4:3), pp 197-229.

Shapiro, S. L., Schwartz, G. E., and Bonner, G. 1998. "Effects of mindfulness-based stress reduction on medical and premedical Students," *Journal of Behavioral Medicine* (21:6), pp 581-599.

Simon, S. J., Grover, V., Teng, J., and Whitcomb, K. 1996. "The relationship of information system training methods and cognitive ability to end-user satisfaction, comprehension, and skill transfer: A longitudinal field study," *Information Systems Research* (7:4), pp 466-490.

Speier, C. 2006. "The influence of information presentation formats on complex task decision-making performance," *International Journal of Human-Computer Studies* (64:11) 11//, pp 1115-1131.

Srikwan, S., and Jakobsson, M. 2008. "Using cartoons to teach internet security," *Cryptologia* (32:2), pp 137-154.

Symantec. 2014. "Internet Security Threat Report 2014. Volume 189," Symantec.

Taylor, P. J., Russ-Eft, D. F., and Chan, D. W. L. 2005. "A Meta-Analytic Review of Behavior Modeling Training," *Journal of Applied Psychology* (90:4), pp 692-709.

Teasdale, J. D., Williams, J. M. G., Soulsby, J. M., Segal, Z. V., Ridgeway, V. A., and Lau, M. A. 2000. "Prevention of Relapse/Recurrance in Major Depression by Mindfulness-Based Cognitive Therapy," *Journal of Consulting and Clinical Psychology* (68:4), pp 615-623.

Tractinsky, N., and Meyer, J. 1999. "Chartjunk or goldgraph? Effects of persenataion objectives and content desirability on information presentation: effects of presentation objectives and content desirability on information presentation," *MIS Q.* (23:3), pp 397-420.

Vance, A., Elie-Dit-Cosaque, C., and Straub, D. W. 2008. "Examining trust in information technology artifacts: the effects of system quality and culture," *Journal of Management Information Systems* (24:4), pp 73-100.

Vessey, I., and Galletta, D. 1991. "Cognitive Fit: An Empirical Study of Information Acquisition," *Information Systems Research* (2:1), pp 63-84.

Vishwanath, A., Herath, T., Chen, R., Wang, J., and 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), pp 576-586.

Vrij, A. 2006. "Nonverbal communication and deception," in *The Sage Handbook of Nonverbal Communication.,* V. Manusov and M. L. Patterson (eds.), Sage Publications, Inc: Thousand Oaks, CA, pp. 341-359.

Webber, C., Lima, M. d. F. W. d. P., and Hepp, F. 2012. "Testing phishing detection criteria and methods " in *Frontiers in Computer Education,* S. Sambath and E. Zhu (eds.), Springer Berlin / Heidelberg, pp. 853-858.

Werts, C. E., Linn, R. L., and Joreskog, K. 1974. "Interclass Reliability Estimates: Testing Structural Assumptions," *Educational and Psychological Measurement* (34:1), pp 25-33.

Wright, R., Chakraborty, S., Basoglu, A., and Marett, K. 2010a. "Where did they go right? Understanding the deception in phishing communications," *Group Decision and Negotiation* (19:4), pp 391-416.

Wright, R. T., Campbell, D. E., Thatcher, J. B., and Roberts, N. 2012. "Operationalizing Multidimensional Constructs in Structural Equation Modeling: Recommendations for IS Research," *Communications of the Association for Information Systems* (40), pp 367-412.

Wright, R. T., Jensen, M. J., Thatcher, J. B., Dinger, M., and Marett, K. Forthcoming. "Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance," *Information Systems Research* (Forthcoming).

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

Yi, M. Y., and Davis, F. D. 2001. "Improving computer training effectiveness for decision technologies: Behavior modeling and retention enhancement," *Decision Sciences* (32:3), pp 521-544.

Zmud, R. W., Shaft, T., Zheng, W., and Croes, H. 2010. "Systematic differences in firm’s information technology signaling: Implications for research design," *Journal of the Association for Information Systems* (11:3), p 1.

1. Federal Trade Commission: http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm;

   Microsoft: http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx;

   Chase Bank: https://www.chase.com/ccp/index.jsp?pg\_name=ccpmapp/privacy\_security/fraud/page/phishing

   Anti-Phishing Working Group: http://www.antiphishing.org/consumer\_recs.html [↑](#footnote-ref-2)
2. http://www.antiphishing.org/consumer\_recs.html [↑](#footnote-ref-3)
3. The university username and password grant access to university email and university resources (e.g., central IT resources, human resource records, academic records). [↑](#footnote-ref-4)
4. The name of the university has been withheld to protect the privacy of the participants of the university. [↑](#footnote-ref-5)
5. http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm [↑](#footnote-ref-6)
6. http://www.antiphishing.org/consumer\_recs.html [↑](#footnote-ref-7)
7. https://www.chase.com/ccp/index.jsp?pg\_name=ccpmapp/privacy\_security/fraud/page/phishing [↑](#footnote-ref-8)
8. The identification practice and knowledge test were scored out of 4. The question about the learning was “This training helped me learn how to identify phishing messages.” and was scored on a 5 point scale with Strongly Disagree and Strongly Agree as the end points. [↑](#footnote-ref-9)
9. Composite reliability scores were calculated as (Σλi)2/[(Σλi)2 + ΣiVar(εi)] where λi is the indicator loading and Var(εi) = 1- λi2. [↑](#footnote-ref-10)
10. The range is 1-5 with Strongly Agree and Strongly Disagree as endpoints. The items are reported in Appendix A under the phishing identification expertise. [↑](#footnote-ref-11)