Information Systems Research

Publication details, including instructions for authors and subscription information:
http://pubsonline.informs.org

Coping Responses in Phishing Detection: An Investigation of Antecedents and Consequences

Jingguo Wang, Yuan Li, H. Raghav Rao

To cite this article:
Jingguo Wang, Yuan Li, H. Raghav Rao (2017) Coping Responses in Phishing Detection: An Investigation of Antecedents and Consequences. Information Systems Research 28(2):378-396. https://doi.org/10.1287/isre.2016.0680

http://pubsonline.informs.org/journal/isre/

INFORMATION SYSTEMS RESEARCH
Vol. 28, No. 2, June 2017, pp. 378–396
ISSN 1047-7047 (print), ISSN 1526-5536 (online)

Coping Responses in Phishing Detection: An Investigation of Antecedents and Consequences

Jingguo Wang,[a] Yuan Li,[b] H. Raghav Rao[c, d]

[a] Information Systems and Operations Management, College of Business, University of Texas at Arlington, Arlington, Texas 76019; [b] Department of Management Information Systems, College of Business and Management, University of Illinois at Springfield, Springfield, Illinois 62703; [c] Department of Information Systems and Cyber Security, College of Business, University of Texas at San Antonio, San Antonio, Texas 78249; [d] Department of Computer Science, University of Texas at San Antonio, San Antonio, Texas 78249

Contact: jwang@uta.edu (JW); yli295@uis.edu (YL); hr.rao@utsa.edu (HR)

Received: June 11, 2015
Revised: March 24, 2016; September 19, 2016
Accepted: October 10, 2016
Published Online in Articles in Advance: April 17, 2017

https://doi.org/10.1287/isre.2016.0680

Abstract. This study investigates users' coping responses in the process of phishing email detection. Three common responses are identified based on the coping literature: task-focused coping, emotion-focused coping (i.e., worry and self-criticism), and avoidance coping. The three responses are used to conceptualize a higher-order construct, coping adaptiveness, that resides on a continuum between maladaptive coping and adaptive coping (manifested as increased task-focused coping and decreased emotion-focused coping and avoidance coping). Drawing on the extended parallel process model and behavioral decision-making literature, this paper examines the antecedents (i.e., perceived phishing threat, perceived detection efficacy, and phishing anxiety) and behavioral consequences (i.e., detection effort and detection accuracy) of coping adaptiveness. A survey experiment with 547 U.S. consumers was conducted. The results show that perceived detection efficacy increases coping adaptiveness. Partially mediated by phishing anxiety, perceived phishing threat decreases coping adaptiveness. Coping adaptiveness positively impacts the two objective measures in the study, detection effort and detection accuracy. The results also suggest that coping adaptiveness and detection effort have different effects on false positives compared to false negatives: detection effort fully mediates the effect of coping adaptiveness on false positive rate (or detection accuracy related to legitimate emails), but has no impact on false negatives (or detection accuracy related to phishing emails), unlike coping adaptiveness. A post hoc analysis on coping responses reveals two patterns of coping among subjects, throwing more light on coping in phishing detection. Theoretical and practical implications are discussed.

History: Sabyasachi Mitra, Senior Editor; Alessandro Acquisti, Associate Editor.
Funding: This research was supported by the National Science Foundation under [Grants SES-1227353 and, in part, SES-1420758 and SES-1419856].
Supplemental Material: The online appendix is available at https://doi.org/10.1287/isre.2016.0680.

Keywords: information security • phishing • coping adaptiveness • the extended parallel process model • detection effort • detection accuracy

1. Introduction

Phishing attacks impose significant threats to businesses and individuals (Caputo et al. 2014, Symantec 2014). Emails have been the primary attack vectors for phishers to distribute their bait and set up hooks (APWG 2014, RSA 2012). Technological measures such as spam filters and security toolbars are used to block, filter, and spread alerts regarding phishing emails at the gateway. However, there is no perfect technological defense, since scammers move one or two steps ahead of technologies, making the latter less effective (Lee and Song 2007, Gupta and Kumaraguru 2014). Recently, email authentication standards such as domain-based message authentication, reporting, and conformance (DMARC) have been created to help authenticate the sources of emails. Yet the success of such defense depends on the accuracy of DMARC records, and the cooperation from Internet service providers. For those phishing emails that pass a technological defense and reach one's email in-box, the burden of detecting the emails transfers to the shoulders of the person.

Humans are an integral part, rather than a secondary constraint, of information security. Any number of security countermeasures in an organization may be futile if the person behind the keyboard falls for a phish (Hong 2012). Understanding how individuals respond to and detect phishing attacks is important to mitigate the associated security risks. Prior studies in phishing generally find that to detect phishing emails, individuals rely on information cues such as the sources of emails, grammar and spelling, email titles, and other design features or content (Anandpara et al. 2007, Dhamija et al. 2006, Downs et al. 2007,

Wright et al. 2014). Via the lens of information processing, a number of studies (see Online Appendix A) have examined how those information cues can be recognized (Dhamija et al. 2006, Downs et al. 2007, Vishwanath et al. 2011, Wang et al. 2012, Wright et al. 2014). Nevertheless, studies show that people often ignore information cues (even security alerts) or fail to deeply examine email content, leading to misjudgment and falling prey to phishing (Dhamija et al. 2006, Mohebzada et al. 2012, Pattinson et al. 2012).

A way to improve users' phishing detection ability is through training (Kumaraguru 2009; Kumaraguru et al. 2008, 2010; Sheng et al. 2007). In the past few years, there has been a significant movement in the corporate world, as part of a phenomenon known as the "human-in-the-loop" (Cranor 2008, Liu et al. 2011), to train users to spot phishing attacks. Most training programs, however, treat humans' process of phishing detection as a black box by viewing phishing knowledge and efficacy as the input and detection accuracy as the output (Wright and Marett 2010). It remains largely unclear how the knowledge that is learned and efficacy that is raised effectively transfer to outcomes in phishing detection. We contend in this study that cognitive and behavioral responses in managing phishing detection could essentially influence the effective transfer of the input (e.g., threat awareness and detection efficacy) to the output (e.g., detection accuracy). Detection of phishing attacks can be cognitively demanding (Vishwanath et al. 2011, Wang et al. 2012). In addition, users may experience negative emotional arousal due to the worry of being victimized (Liang and Xue 2009). Proper cognitive and behavioral responses in managing the demand for recognizing phishing (or, proper coping with phishing) could play a critical role so that users can focus on detection but not withdraw or be distracted by negative emotional arousal.

Specifically, this study investigates three research questions: (1) what coping responses do users engage in during their process of detecting phishing, (2) what factors influence users' coping responses, and (3) how do coping responses impact phishing detection performance? Based on coping literature on cognitively demanding tasks (Matthews and Campbell 1998, Matthews et al. 2002), three common coping responses are identified: task-focused coping, emotion-focused coping, and avoidance. The three coping responses are not exclusive, but coexist (Popova 2012, Witte and Allen 2000, Wright 2010). We thus argue for a higher-order coping construct reflecting coping adaptiveness, residing on a continuum between maladaptive coping and adaptive coping (manifested as increased task-focused coping and decreased emotion-focused coping and avoidance coping). Such a formulation provides a parsimonious model of coping responses. Drawing on the extended parallel process model (Witte and Allen 2000), we investigate the effect of perceived phishing threat, perceived detection efficacy, and anxiety of being phished on coping adaptiveness. Integrating the behavioral decision-making literature, we develop a research model to examine the impact of coping adaptiveness on detection effort and detection accuracy.

A survey experiment on 547 U.S. consumers from a broad demographic base was carried out to test our research model. The results show that perceived detection efficacy increases coping adaptiveness in phishing detection. Perceived phishing threat has the effect of decreasing coping adaptiveness. This effect is partially mediated by phishing anxiety. Coping adaptiveness positively impacts both detection effort and accuracy. Our results also suggest that for legitimate business emails, detection effort fully mediates the effect of coping adaptiveness on detection accuracy (or, conversely, on false positive rate); for phishing emails, detection effort has no impact on accuracy (or, conversely, on false negative rate), but coping adaptiveness has an impact. A post hoc analysis on coping responses among subjects reveals two patterns (we name them *adapters* and *maladapters*), throwing more light on coping with phishing attacks. A novel aspect of this study is to employ a survey experiment to help facilitate participants' engagement in the phishing detection process. Such an approach enables us to capture users' coping responses in their process of phishing detection and the associated outcomes, which otherwise could be hard to solicit with a survey or a mock (or simulated) phishing attack. Detection effort and detection accuracy (the outcome variables) were objectively measured in the experiment, while other principle constructs relied on self-reported measures. Linking the self-reported data to the objectively measured data for hypothesis testing helps avoid common method bias, which could be a challenging issue for studies that rely only on self-reported data.

This paper is organized as follows. Section 2 introduces the theoretical background and develops the research model. Section 3 details the research design and data collection approach. Section 4 presents the results of data analyses. Section 5 discusses contributions, limitations, and future research.

2. Theory and Hypotheses

2.1. Theoretical Background

2.1.1. Coping Responses. Coping plays an important role in individuals' reactions to demanding situations (Endler and Parker 1990; Matthews et al. 2002, 2006; Matthews and Campbell 1998). Understanding coping responses helps us to discover mechanisms to better deal with such situations and to improve well-being. There have been a number of studies in information security that follow the protection motivation theory (PMT) (Rogers 1975) to understand how users

cope with security threats (for a comprehensive review, see Boss et al. 2015). Most studies focus on desired responses that are adaptive in nature, such as avoidance of information technology (IT) threats (Liang and Xue 2009, 2010) and adoption of protective behavior (Boss et al. 2015, Johnston and Warkentin 2010, Johnston et al. 2015, Lai et al. 2012). In addition, most researchers investigate how threat appraisal and coping appraisal influence one's protective behaviors, and only a few have started to explore the role of negatively valenced emotions (such as fear, anxiety, and worry) in coping (Boss et al. 2015). This leaves two gaps in the theory. First, as both adaptive and maladaptive responses exist in individuals' coping with demanding events (Endler and Parker 1990, Witte and Allen 2000), both types of responses need to be investigated to understand how people actually deal with security threats. Second, as negatively valenced emotions are an integral part of coping theories (Boss et al. 2015, Popova 2012, Witte and Allen 2000), these factors need to be incorporated to understand how they influence coping responses to security attacks. In this section, we bridge the first gap by identifying coping responses for phishing detection based on the psychological literature and conceptualizing coping adaptiveness for model development. In the next section, we draw on the extended parallel process model (EPPM) (Witte and Allen 2000) to introduce the role of phishing anxiety.

Dozens of coping responses have been examined in the psychological literature (Endler and Parker 1990). Based on an extensive review, Endler and Parker (1990) propose three fundamental dimensions of coping (Matthews et al. 1999), which include task-focused coping, emotion-focused coping, and avoidance coping. *Task-focused coping*, also known as *problem-focused coping*, aims to directly address the problem itself and actively take steps to deal with the stressful situation. Engaging in this coping response, an individual attempts to formulate and execute a plan of action to deal with task demands, change external reality, and resolve the problem directly. *Emotion-focused coping* attempts to deal with the task or stressor by changing one's feelings or thoughts about it. It includes both negatively toned strategies (such as worry and self-criticism) and positively toned strategies (such as positive thinking or reappraisal), but researchers show that worry and self-criticism often dominate this type of coping in empirical tests (Endler and Parker 1990, Matthews and Campbell 1998). Such a coping response tends to activate self-discrepancies and elevate both distress and worry (Matthews et al. 2002, Matthews and Campbell 1998). *Avoidance coping* involves withdrawal from task-related activities and diversion of one's attention from the problem to be addressed. Engaging in avoidance coping, an individual adopts strategies that help avoid stressful situations rather than solve them.

To measure one's coping responses in dealing with particular tasks, Matthews et al. (2002, 2006) and Matthews and Campbell (1998) developed an instrument for immediate posttask assessment, following the three dimensions suggested by Endler and Parker (1990). Task-focused coping is reflected by planned action (e.g., "made every effort to achieve my goals"), emotion-focused coping is reflected by self-criticism and worry (e.g., "worried about my inadequacies"), and avoidance coping is reflected by withdrawal of attention from the task and giving up (e.g., "acted as though the task was not important"). The instrument has been adopted in a number of studies on individuals' coping responses in demanding tasks such as simulated driving, working memory, and other information processing tasks (Matthews et al. 1999, 2002, 2006, 2010; Shaw et al. 2010).

This study adopts the instrument developed by Matthews et al. (2002, 2006) and Matthews and Campbell (1998). Table 1 lists the three coping responses, their interpretations in terms of phishing detection, and the measurement items. The items aim to measure the coping responses that subjects engage in during their detection process. They were presented to the

Table 1. Coping Responses in Phishing Email Detection

Coping responses	Scenario of phishing detection	Measurement items (Matthews et al. 2002, 2006; Matthews and Campbell 1998)[a]
Task-focused coping	When engaging in task-focused response, users aim to actively recognize phishing emails. For example, users could thoughtfully analyze cues presented in an email and decide its legitimacy.	I made every effort to achieve my goals. I was single-minded and determined in my effort to overcome any problems. I concentrated hard on doing well.
Emotion-focused coping	When engaging in emotion-focused response, users may self-criticize their inadequacies and worry about their outcomes in the process of phishing detection.	I worried about my inadequacies. I blamed myself for not doing better. I blamed myself for not knowing what to do.
Avoidance coping	When engaging in avoidance, users withdraw their effort and divert their attention from the task of phishing detection.	I acted as though the task was not important. I did not take the task too seriously. I decided there was no point in trying to do well.

[a]The respondents are asked to indicate to what extent they agree with each of the statements regarding the goals of judging the emails (i.e., differentiating phishing emails from legitimate business emails) in the survey.

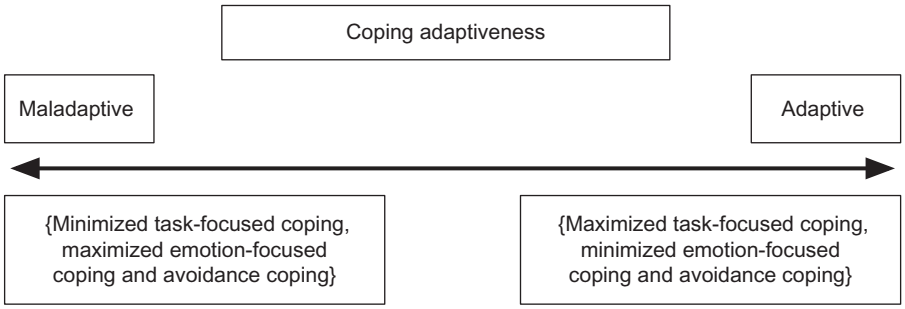
subjects after they just finished differentiating phishing emails from legitimate business emails in the survey experiment. We describe the design of the survey experiment in detail in Section 3.1.

Prior studies in coping have in general suggested the positive effects of task-focused coping and the negative effects of emotion-focused and avoidance coping on outcomes, especially when individuals' effortful responses may improve a threatening situation (Lazarus and Folkman 1984, Zeidner and Saklofske 1996). Although task-focused coping is negatively related to emotion-focused and avoidance coping, the three are not exclusive; rather, people use a mixture of all three coping responses when dealing with a task or event (Popova 2012, Witte and Allen 2000, Wright 2010), and their coping strategies or the mix of the responses may vary with the task as well as individual and contextual factors (Matthews et al. 2002, 2006; Matthews and Campbell 1998). Following Rippetoe and Rogers (1987), we suggest that adaptive coping in the scenario of phishing detection is characterized by increased task-focused coping and decreased emotion-focused and avoidance coping, and conversely, maladaptive coping is characterized by decreased task-focused coping and increased emotion-focused and avoidance coping. We therefore conceptualize a higher-order coping construct that consists of the three coping responses and name it *coping adaptiveness*, which resides on a continuum from maladaptive coping to adaptive coping (Figure 1).

2.1.2. The Extended Parallel Process Model. To study the particular antecedents of coping responses, we draw on the EPPM (Popova 2012, Witte and Allen 2000), which is an extension of the PMT. The model proposes that (1) individuals' cognitive appraisals of the situational demands (i.e., perceived threat) and personal coping resources (i.e., perceived efficacy) influence their coping responses in the situation, (2) negative emotional arousal plays an important role in determining the responses, and (3) reacting to the threats, individuals may engage in the danger control process and/or the fear control process. Specifically, an individual goes through two appraisals in a demanding situation (e.g., differentiating legitimate business emails from phishing emails) before responding. First is the threat appraisal, referring to the individual's judgment of the level of threat in the situation. The output is called *perceived threat*, defined as the subjective evaluation of the threat presented in the situation. It comprises two dimensions—*perceived severity* of the threat (i.e., the belief about the magnitude or significance of the threat and the gravity of its consequences) and *perceived susceptibility* to the threat (i.e., the belief about the probability of personally experiencing the threat)—which together determine the extent of perceived threat (Witte 1992). The second appraisal, called the coping appraisal, deals with the individual's judgment of the ability to handle the threat and is measured by *perceived efficacy*, defined as cognitions about the effectiveness, feasibility, and ease with which a response alleviates or helps in avoiding a threat. It also comprises two dimensions—*perceived response efficacy* (i.e., the belief about how effective the response will be in averting a threat) and *perceived self-efficacy* (i.e., the belief about one's ability to carry out the response)—which together determine perceived efficacy (Witte 1992). The EPPM suggests that an individual will first appraise the situational threat, and only when a noticeable threat is perceived will she appraise the efficacy to deal with the threat.

It should be noted that perceived response efficacy and perceived self-efficacy must work in tandem to influence coping responses, so the combination of the two into a single construct known as *coping efficacy* is quite common in the literature (Witte and Allen 2000, Floyd et al. 2000, Popova 2012). For example, past research on online security has used a single construct to measure coping appraisal within a specific task context (Zhang and McDowell 2009). We adopt this approach, particularly, merging response efficacy into self-efficacy, for two reasons. First, response efficacy represents the expectancy that the recommended protective behavior yields desired outcomes (Liang and Xue 2009); for example, antimalware (or antispyware) software provides effective protection against malware attacks (Johnston and Warkentin 2010). In the area of phishing detection, response efficacy reflects the expectancy of coping responses that help to detect

Figure 1. Coping Adaptiveness



phishing emails. The expectancy of coping outcomes is directly manipulated in the research design in this study, as the subjects are explicitly required to differentiate phishing emails from legitimate business emails. Therefore, response efficacy can be treated as a constant. This is similar to the approach that Hann et al. (2007) applied in their study on behavioral expectancy in information privacy. Second, our study does not address individuals intention to adopt a recommended response, but their cognitive and behavioral responses in the process of phishing email detection (via immediate posttask assessment). The responses available for an individual to choose in the process of detection will be largely limited by the level of efficacy an individual has regarding phishing detection (Bandura 1982, Rippetoe and Rogers 1987). The level of efficacy of phishing detection also implies how well an individual can respond in the detection process. Therefore, a separate measurement of response efficacy and self-efficacy regarding different responses in phishing detection is deemed unnecessary. We conceptualize perceived efficacy as *perceived detection efficacy*, referring to one's belief about her ability to recognize phishing emails.

Two coping processes, including danger control and fear control, are proposed in the EPPM. Danger control involves coping responses that engage in protective behavior, or task-focused coping, to reduce or avert the threat. Fear control involves coping responses to handle the fearful feeling or emotion (through denial, avoidance, reactance, etc.) engendered by threats (Popova 2012). Empirical studies on the EPPM show that these two processes are not exclusive but may coexist (Witte and Allen 2000). Wright (2010) argues, citing Witte and Allen (2000), that a negative correlation exists between the two, suggesting that attempts to control the threat and to cope with emotional arousal operate at least somewhat in parallel. Therefore, as mentioned above, we propose to use a second-order construct to capture both types of responses and reflect the adaptiveness of coping.

Another important proposition of the EPPM deals with the roles of negatively valenced emotion (e.g., frightened, concerned, scared, distressed, or anxious; Popova 2012, Witte 1992). It suggests that such arousal results in the fear control process. In the context of this study, we use the term "phishing anxiety" to refer to such an emotion or feeling regarding the risk of being victimized by phishing attacks. We argue that individuals' anxiety about being victimized by a threat is elicited when the threat is perceived to be significant and personally relevant, and is heightened and intensified with the perception of low coping efficacy. In the case of phishing attacks, an individual's anxiety of being phished increases when phishing attacks are perceived to be relevant and significant (Caputo et al. 2014, Jakobsson and Myers 2006). Phishing anxiety may increase coping maladaptiveness in the process of detection.

2.1.3. Coping Outcomes. Coping responses are expected to explain outcome variability among individuals (Lazarus and Folkman 1984, Matthews and Campbell 1998, Witte 1992). In this study, the outcome variables are individuals' mental or cognitive effort expended in the detection task (referred to as detection effort) and the percentage of emails correctly recognized (referred to as detection accuracy). Effort and accuracy are two main variables used to understand behavioral decision making such as judgmental tasks (Johnson and Payne 1985, Payne 1982). Todd and Benbasat (1999, 2000) show that the trade-offs between effort and accuracy are common to decision makers, and effort saving is a general tendency in the decision or judgmental process. Mechanisms that aim to enhance detection accuracy must first address the issue of detection effort. We investigate how coping responses are related to these two aspects in phishing detection.

2.2. Hypothesis Development

2.2.1. Antecedents of Coping Responses. Drawing on the EPPM, we analyze three antecedents of coping responses: perceived threat of phishing attacks, perceived detection efficacy, and phishing anxiety. We first examine perceived threat of phishing attacks, which consists of perceived susceptibility to phishing attacks and perceived severity of phishing victimization. In line with the EPPM, perceived susceptibility to phishing attacks is the extent to which an individual perceives the likelihood of herself falling prey to phishing attacks, and perceived severity of phishing victimization is the extent to which an individual perceives the negative consequences caused by being a victim of phishing attacks. The EPPM suggests that the effects of both are additive (Witte 1992, Witte and Allen 2000): when individuals believe that they are vulnerable to phishing attacks and that the consequence of being compromised is severe, perceived threat of the attacks will result. In the area of information security, it has been suggested that perceived susceptibility and perceived severity increase the extent to which an individual perceives malicious IT as dangerous or harmful (Liang and Xue 2009, 2010).

For phishing attacks, we argue that, on one hand, perceived threat induces one's protection motivation to deal with the threat, as suggested by both PMT and the EPPM and evidenced in the information security literature (Boss et al. 2015, Johnston et al. 2015). We therefore expect that perceived threat leads to increased task-focused coping in the process of phishing detection. On the other hand, perceived threat also increases emotion-focused and avoidance coping, as in the fear control process outlined in the EPPM. This

happens, following the EPPM, when perceived threat arouses the fearful feeling of the attacks and activates the defensive motivation for emotional adjustment, so that emotion-focused and avoidance coping can follow (Popova 2012). In the context of mitigating identity theft risks, Anandarajan et al. (2012) show that perceived severity has a stronger impact on maladaptive coping (i.e., giving up or withdrawing) than on adaptive coping (i.e., using risk reduction methods), while perceived vulnerability is insignificant. Therefore, although perceived threat increases the likelihood to engage in all three coping responses in phishing detection, it could possibly increase emotion-focused and avoidance coping more than task-focused coping, resulting in decreased coping adaptiveness. Therefore, we propose the following:

Hypothesis 1 (H1). *Perceived phishing threat decreases coping adaptiveness in phishing detection.*

Prior studies suggest that individuals rely on a variety of information cues embedded in emails to identify phishing attacks (Anandpara et al. 2007, Dhamija et al. 2006, Downs et al. 2007). Individuals may differ in their perceived ability to exercise these heuristic decision strategies. Perceptions of phishing detection efficacy can determine coping responses to be adopted when an individual confronts a phishing attack. Phishing detection efficacy may increase task-focused coping, as an individual knows what to do to detect phishing attacks (Witte 1992, Witte and Allen 2000). Meanwhile, it may reduce the likelihood to engage in emotion-focused coping or avoidance coping, as individuals with high perceived efficacy are more confident in taking protective action instead of engaging in worry, self-criticism, or avoidance in dealing with phishing detection (Bandura 1982, Rippetoe and Rogers 1987). Therefore, we propose the following:

Hypothesis 2 (H2). *Perceived detection efficacy increases coping adaptiveness in phishing detection.*

We further propose a potential relationship between perceived threat and perceived detection efficacy. As suggested by the EPPM, threat appraisal and coping appraisal are an ordered process in that threat appraisal takes place first and then leads to coping appraisal: if a person perceives a potential threat, she will evoke the coping appraisal to find the appropriate countermeasure; if a potential threat is not perceived or is too low, the person will not initiate the appraisal of coping strategies. As perceived threat increases, the person will question her ability to adequately cope with the threat; on the other hand, if the perceived threat decreases, the person will feel more confident in her ability to deal with the threat. This negative relationship was also evidenced in Johnston and Warkentin (2010) in the context of investigating one's intention to use antispyware software. Therefore, we propose the following:

Hypothesis 3 (H3). *Perceived phishing threat decreases perceived detection efficacy.*

2.2.2. Phishing Anxiety. Perceived phishing threat and perceived detection efficacy do not only have direct impacts on coping responses but also have indirect impacts via the emotional experience they engender: phishing anxiety. Following the EPPM (Witte 1992, Witte and Allen 2000), we argue that when individuals believe that they are vulnerable to phishing attacks and that the consequence of being compromised is severe, phishing anxiety will increase and influence the subsequent choice of coping responses. The fearful feeling is triggered by the cognitive process in threat appraisal. The greater the threat a person perceives, the more fearful she could become. In the area of information security, it has been suggested that perceived susceptibility and perceived severity increase the extent to which an individual perceives malicious IT as dangerous or harmful (Liang and Xue 2009, 2010; Boss et al. 2015). Therefore, we propose the following:

Hypothesis 4 (H4). *Perceived phishing threat increases phishing anxiety.*

As mentioned above, individuals rely on a variety of cues embedded in emails to identify phishing attacks, and they differ in their perceived ability to exercise these heuristic decision strategies. The perception of low efficacy for detecting phishing emails may heighten and intensify the anxiety that phishing attacks cannot be avoided; by contrast, the perception of high efficacy in detecting phishing emails decreases phishing anxiety. If an individual believes that she can effectively recognize phishing emails appearing in the mailbox, she may not perceive phishing attacks as alarming. In the context of information security, it has been argued that an individual's belief in her own ability to take recommended precautions contributes directly to activating the necessary affect toward taking security precautions (Anderson and Agarwal 2010). In the context of computer use, computer self-efficacy has been found to exert significant influences on individuals' emotional reactions to computers (i.e., affect and anxiety; Compeau and Higgins 1995, Wilfong 2006). Therefore, we propose the following:

Hypothesis 5 (H5). *Perceived detection efficacy decreases phishing anxiety.*

In terms of the behavioral consequence, the EPPM suggests that negative emotional arousal increases emotion-focused and avoidance coping (Witte 1992). In the context of phishing detection, phishing anxiety activates the defensive motivation for emotion control in the process of phishing detection, and thus

causes an individual to engage in emotion-focused and avoidance coping. In the area of computer use, it has been found that an increased level of negative affect such as computer anxiety leads to a decreased level of computer or IT use in performing one's job (Beaudry and Pinsonneault 2010, Compeau and Higgins 1995, Wilfong 2006). Therefore, we propose the following:

Hypothesis 6 (H6). *Phishing anxiety decreases coping adaptiveness in phishing detection.*

2.2.3. Consequences of Coping Responses. We analyze how coping responses influence detection effort and detection accuracy. For detection effort, the coping literature suggests that the use of task-focused coping is reciprocally linked to task engagement, which is ones' commitment to investment of effort in task performance (Matthews et al. 2010). Matthews et al. (2010) found that more engaged individuals were more likely to appraise the task as controllable, more likely to use task-focused coping, and less likely to use avoidance coping (which commits no effort to the task). A further empirical study on demanding tasks confirmed the positive relationship between task-focused coping and effort as well as the negative relationship between avoidance and effort (Matthews and Campbell 1998). Avoidance coping inhibits the motivation and energy for protection (Rippetoe and Rogers 1987) and withdraws attention from the task (Matthews et al. 1999). In terms of phishing detection, this implies that task-focused and engaged users aim to actively recognize phishing emails by, for example, thoughtfully analyzing the cues presented in the emails and deciding their legitimacy, while avoidance users do not exert such efforts.

People engaged in emotion-focused coping tend to address the issue by redirecting emotions or blaming themselves rather than actively searching for solutions (Matthews et al. 2007). With such coping responses in detecting phishing emails, individuals may be less likely to engage in effortful and self-critical search for reasons to justify their judgment (Lerner and Tetlock 2003); instead, they reduce the effort directed toward comprehending and inspecting an email so as to reach a judgment in phishing email detection. Note that studies on the relationship between emotion-focused coping and effort have not been conclusive (Matthews et al. 1999, Matthews and Campbell 1998). Matthews and Campbell (1998) argue that the result may be influenced by the particular task, and clear evidence exists for the impact of emotion-focused coping on tasks that are demanding and have personal stakes. We suggest that as phishing detection is a demanding task with high personal stakes, it will engender a negative impact of emotion-focused coping on effort. Therefore, we propose the following:

Hypothesis 7 (H7). *Adaptive coping increases detection effort.*

For detection accuracy, we expect similar effects of coping responses. On one hand, task-focused coping enhances task engagement, including energetic arousal, task interest, success motivation, and concentration (Matthews et al. 2010). These factors help the individual to commit to the cognitive process to address the demanding situation, therefore leading to better detection accuracy. On the other hand, emotion-focused coping causes high mental demands (such as tension and worry) and frustration, making one prone to errors and difficulties in attending to the task (Matthews and Campbell 1998), and leading to a negative impact on detection accuracy. Although avoidance coping may help to reduce tension, it commits no effort to effectively address the demanding task, but increases task-irrelevant thinking (Matthews et al. 1999). Its association with lower detection accuracy naturally holds. Therefore, we propose the following:

Hypothesis 8 (H8). *Adaptive coping increases detection accuracy.*

There is also a potential relationship between detection effort and detection accuracy, as the literature shows that the more cognitive effort an individual expends, the better the decision reached (Johnson and Payne 1985, Payne 1982). Increased cognitive effort has been found to decrease susceptibility to a host of common biases, such as oversensitivity to the order of appearance of the information (Webster et al. 1996) and overconfidence (Siegel-Jacobs and Yates 1996). Increases in cognitive effort have also been found to attenuate strategy-based errors (Arkers 1991). In phishing detection, with increased detection effort, individuals may be able to examine a wider range of conceivably relevant cues and more closely look at the cues they utilize in their judgmental process. They may be more likely to discover inconsistent cues, thereby noting the abnormality of a phishing email and raising suspicion. They may also become more aware of their cognitive processes, and consequently have fewer decision errors. Therefore, we propose the following:

Hypothesis 9 (H9). *Detection effort increases detection accuracy.*

Hypotheses 7–9 together suggest a mediating effect of detection effort on the relationships between coping adaptiveness and detection accuracy. We argue that the effect differs between the detection of legitimate emails (or, conversely, false positives) and the detection of phishing emails (or, conversely, false negatives). From an error management point of view (Masip et al. 2005),

failing to detect a phishing email (i.e., a false negative) may be more harmful than wrongfully marking a legitimate email as phishing (i.e., a false positive), so that the tendency of trying to catch all phishing emails may lead individuals to be lie biased. Such a bias has been observed for police officers who are more concerned with catching a cheater but less concerned with wrongfully accusing a suspect (Masip et al. 2005). It has also been observed in prior phishing research that some users have increased false positive errors (i.e., marking a genuine email as a phishing email) after training (Anandpara et al. 2007, Kumaraguru et al. 2010, Sheng et al. 2007). In other words, an individual's default assumption in the process of detection regarding an email could be that it is a phishing attack. Only if she has the time, motivation, and energy to think more about the email will it be more credible (Levine 2014, p. 156). Therefore, we propose the following:

Hypothesis 10 (H10). *Detection effort has a stronger effect on detection accuracy related to legitimate business emails (or conversely, false positive rate) than that related to phishing emails (or conversely, false negative rate).*

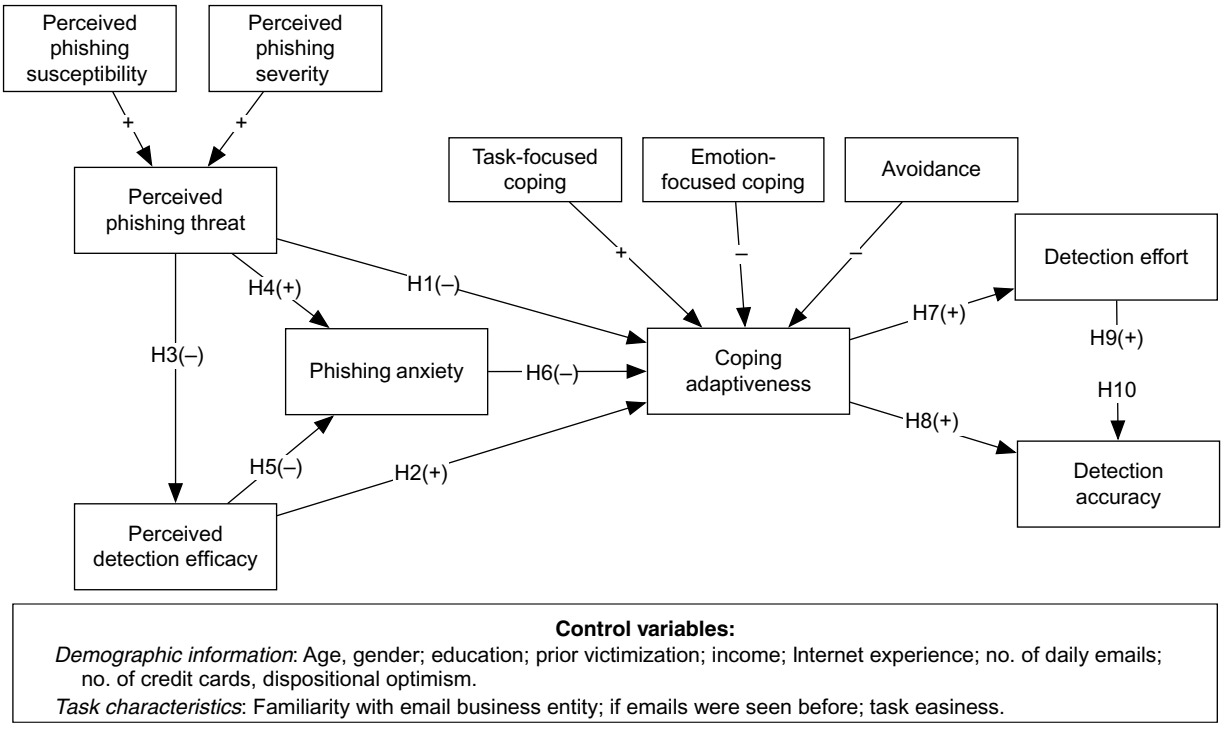
2.2.4. Control Variables. A number of control variables are included in the research model following prior literature in phishing. These variables include individual differential factors such as gender, age, dispositional optimism, education, prior victimization, income level, Internet experience, the number of daily emails received, and the number of credit cards (Jagatic et al. 2007, Piquero et al. 2011, Sheng et al. 2010, Vishwanath et al. 2011), and task characteristics such as how familiar a respondent is with the business entity indicated by an email (Wang et al. 2012), how many emails a respondent felt that she saw before, and how easy it is to recognize the nature of emails included in a judgment task. For example, education, Internet experience, familiarity with a business entity, and knowledge on a related email constitute a person's knowledge level that may influence her detection responses and phishing susceptibility (Downs et al. 2007, Sheng et al. 2010, Vishwanath et al. 2011, Wang et al. 2012). The individual differential factors are controlled for phishing anxiety, and both individual differential factors and task characteristics are controlled for the coping responses, detection effort, and detection accuracy in the study. Figure 2 summarizes our research model and hypotheses.

3. Research Method and Data Collection

3.1. Design of the Survey Experiment

A web-based survey experiment was developed using Qualtrics Research Suite. The survey experiment asked the subjects to differentiate among a mixed set of phishing and legitimate business emails and also self-report their perceptions related to the research constructs (except for detection effort and accuracy, which were objectively measured). This research design is different from that of some prior studies in which mock phishing attacks were sent to users that needed to be detected in the context of their everyday email demands (for example, Dodge et al. 2007, Kumaraguru

Figure 2. Research Model and Hypotheses



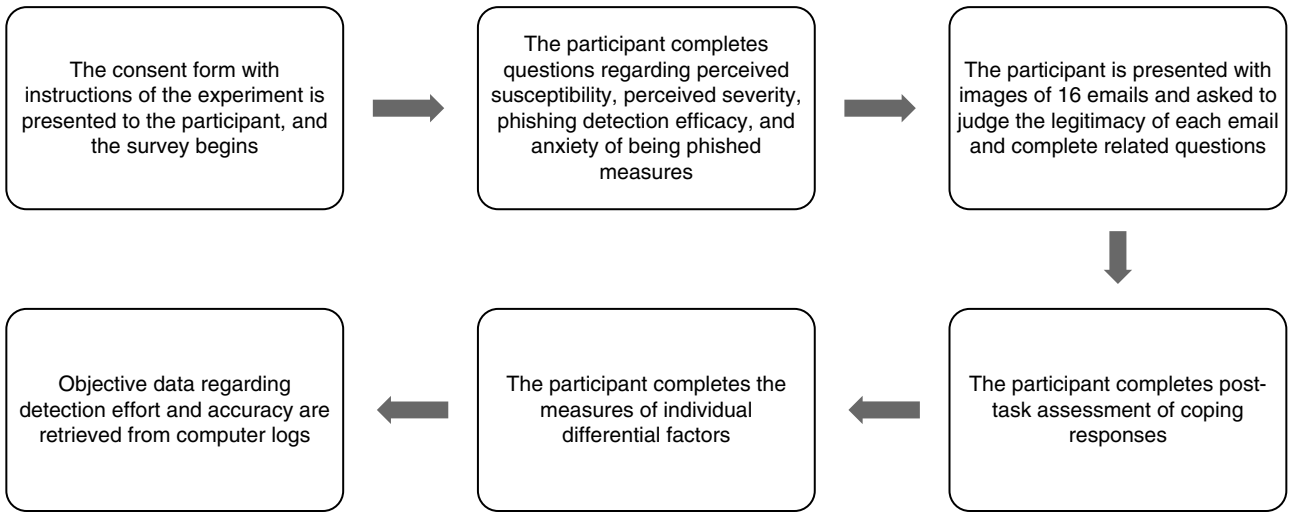
et al. 2008, Mohebzada et al. 2012, Moody et al. 2011, Wright et al. 2014). Because the purpose of this study is to understand how users form their coping responses, which in turn impact detection outcome, the survey experiment has facilitated subjects' engagement in the process of detection. It enables us to capture users' coping responses and measure detection outcomes (including detection effort and detection accuracy) objectively, which otherwise could be difficult to solicit using other methods. The design follows a number of prior studies in understanding phishing susceptibility and training effectiveness as well (for example, Anandpara et al. 2007, Furnell 2007, Pattinson et al. 2012, Sheng et al. 2010, Vishwanath et al. 2011, Wang et al. 2012). Such an approach has also been used in industry practice to help laymen become aware of their ability to detect phishing attacks (see http://www.sonicwall.com/furl/phishing/). In addition, such an experiment design is aligned with prior lab studies in understanding deception detection (Albrechtsen et al. 2009, Hee and Levine 2010, Levine et al. 2006).

The design of the survey experiment is illustrated in Figure 3. First, the consent form with instructions of the experiment was presented to each participant. An excerpt from the consent form is shown in Online Appendix B. It suggests that the purpose of this study is to understand the process of how individuals detect legitimate and phishing emails via judging 16 emails and answering a set of related questions. If the subject believed the email was truly sent from the business entity it claimed to be, "Yes" should have been chosen; if the subject believed the email was from someone pretending to be the business entity it claimed to be (i.e., it was a phishing email pretending to be from a legitimate business entity), "No" should have been chosen.

After acknowledging the consent form, the participants were presented with items measuring perceived susceptibility, perceived severity, perceived detection efficacy, and phishing anxiety in a random order. We did not manipulate the participants' threat and coping appraisal and their emotional arousal regarding phishing attacks, but collected their perceptions that were formed based on their observation of the environment and past experience related with phishing attacks. Subsequently, 16 email images were randomly chosen from a pool of 50 emails and presented to the participants in a sequential manner. The number of emails was determined based on a pretest and pilot study so that most of the participants were able to finish the survey in approximately 15 minutes.

Among the 50 emails in the research pool, half were legitimate business emails and the other half were phishing emails. Such a mix not only maximized the uncertainty in the judgments but also did not make detection accuracy biased toward the users with either lie bias or truth bias (Masip et al. 2005). We focused on business emails sent by, and phishing emails targeting customers of, banks or financial institutions in the United States. In recent years, customers of banks and financial institutions have been heavily targeted by identity thieves for their private information (Hong 2012, RSA 2012). The business emails were collected from banking colleagues' and the authors' email inboxes and also from the public domain, such as http://www.netbanker.com. Most of the phishing emails were collected from public domains (such as http://www.consumerfraudreporting.org, http://www.millersmiles.co.uk/, and http://www.antiphishing.org), and a few were from banking colleagues' and authors' inboxes. The emails (both legitimate and phishing emails) involved major national banks or financial institutions (such as Bank of

Figure 3. Design of the Survey Experiment



America, Chase, Citi, and Discover), regional organizations (such as First Niagara, M&T, and regional credit unions), and online payment and financial service companies (such as PayPal, BillGuard, and Lending Club). A criterion for selecting emails from the public domain for the study was that the text of the email should be clearly legible (as most of the emails were made available in the form of image files) and include information cues such as sender, receiver, time sent, and title. For example, some email images (see the example in Online Appendix B) show a mouseover URL at the bottom of the image if the URL is hidden, and some emails contain an attachment. In addition, all of the images had the senders' email address visible. We changed the receivers' names and email addresses, if they were private, to fictitious names and emails. We did not change the receiver's address if the email had no receiver address shown, was sent to a group (for example, undisclosed recipients), or was clearly not a private email (for example, PayPal as the receiver). In the consent form of the survey, though, we emphasized that all these emails were actual ones except for the removal of the private information.

For each email, each participant was asked to judge whether it was a legitimate email (yes/no), whether she had personally received or seen the email before (yes/no), and how familiar she was with the business entity indicated in the email (a five-point Likert scale). An example of the email along with the three associated questions is presented in Online Appendix B. All 16 emails followed the same presentation format. After the participants finished judging the emails, they were asked to assess the nine items measuring their coping responses to the judgment task. To ensure that task-specific coping responses were captured, we emphasized in the questionnaire that the items were regarding their goal of judging the emails (differentiating phishing emails from legitimate business emails). Finally, each participant completed other measures of individual differential factors. The protocol was pretested with a group of faculty members, doctoral students, undergraduate students, and university administrative staff, and then pilot tested with a small group of undergraduate students following Churchill (1979) before the actual data collection to ensure its clarity and content validity. Minor changes were made in the survey following the feedback gathered from the pretest and the pilot study.

3.2. Measurement

Online Appendix C presents the measurement items for the latent constructs in the research model. We adopted measures from the existing literature and made necessary adaptations to fit them into the research context. Items measuring perceived susceptibility and perceived severity of phishing attacks were adapted from Johnston and Warkentin (2010) and Liang and Xue (2009). Items for perceived detection efficacy were adapted from Chen et al. (2011) and Herath et al. (2012). Items measuring phishing anxiety were adapted from Champion et al. (2004). The items measuring coping response in phishing detection were adapted from the Coping Inventory for Task Stress (Matthews et al. 2002, 2006; Matthews and Campbell 1998). We included three items for task-focused coping, three items for emotion-focused coping, and three items for avoidance coping, each having a loading higher than 0.70. These nine items were presented in random order after a participant completed judgment on the emails.

Detection effort was measured by the time spent in completing the judgmental task (Bettman et al. 1990, Garbarino and Edell 1997). Specifically, we recorded time that elapsed between when an email was shown and when a click was made to answer the question of whether the mail was legitimate or not. We then calculated the mean time for all 16 emails in the group and log-transformed the mean time to improve measurement normality. Detection accuracy was measured by the percentage of correct answers of each participant from the set of 16 emails.

The three task characteristics (as control variables) were measured with aggregated scores from the 16 emails, such as the average of business entity familiarity and the aggregated "seen earlier" measures. For task easiness (i.e., how easy it is to judge the group of emails presented to the participant), we first calculated the easiness of each email based on the percentage of participants who made correct judgments on that email, and then averaged the easiness scores of the 16 emails presented to each participant. We used the aggregated scores of these control variables since the corresponding dependent variables—detection effort and accuracy—were similarly measured by aggregated scores from the 16 emails in the task. Dispositional optimism was assessed by the 10-item Life Orientation Test–Revised scale developed by Scheier et al. (1994), which were aggregated into a single score following the literature. Other demographic factors were measured with single items, including age, gender, education, income, the number of daily emails received, and the number of credit cards in one's wallet. Prior victimization was measured by three dichotomous items aggregated into a single score. Internet experience was measured by six items aggregated into a single score.

3.3. Survey Administration

As mentioned earlier, to provide better external validity of our results, we collected data from a Qualtrics panel drawn from U.S. consumers. We filtered those participants who had never performed any of the following online activities: purchasing products or services online, accessing bank accounts online, paying

Table 2. Summary of Sample Demographics ($N = 547$)

Gender		Education (Continued)	
Male	197	Some high school	11
Female	350	High school graduate	116
Age		Some college	192
Minimum	19	College graduate	146
Maximum	89	Postgraduate	80
Mean	51.62	Ethnicity	
Median	50	White/Not Hispanic	462
Standard deviation	17.89	Black/Not Hispanic	39
Household income		Hispanic	18
Less than $25,000	123	Other/Not Hispanic	28
$25,000–$50,000	190	Number of credit cards in wallet	
$50,000–$75,000	121	1	214
$75,000–$100,000	67	2	134
>$100,000	46	3	98
Education		4	50
Less than high school	2	>4	51

bills online, and buying or selling stocks or mutual funds online. We deemed those individuals foreign to the research context and unsuitable for the study. A total of 547 valid responses were collected from 47 states in the United States. Table 2 summarizes the demographic characteristics of our sample.

4. Data Analysis and Results

We tested the research model using the partial least squares (PLS) method to accommodate the complexity of the model, the use of a formative construct (i.e., perceived threat), and the different types of measurements in the model (Gefen et al. 2011). These factors may cause problems such as inadmissible solutions and factor indeterminacy if the covariance-base structural equation modeling approach is used. In addition, PLS is well suited for the exploratory models and theory development used in this study (Vinzi et al. 2010). We employed SmartPLS 2.0 software (Ringle et al. 2005) and used the bootstrap procedure (with 500 resamples) to estimate the significance of the path coefficients and weights.

4.1. Measurement Validation

We first evaluated the psychometric properties of the latent constructs including perceived susceptibility of phishing attacks, perceived severity of phishing victimization, perceived detection efficacy, phishing anxiety, task-focused coping, emotion-focused coping, and avoidance coping. Their reliability, convergent validity, and discriminant validity were analyzed (Fornell and Larcker 1981). The reliability test showed that an item for the task-focused coping construct had a low item-to-total correlation; this item was dropped from further analysis. Table D1 in Online Appendix D provides the mean values, standard deviations, average variance extracted (AVE), reliability statistics, and correlations of the constructs; descriptive information and correlations of the research constructs (including age and dispositional optimism) are also provided. Item loadings and cross loadings are shown in Table D2 in Online Appendix D. We assessed measurement reliability based on both composite reliability and Cronbach's alpha. As shown in Table D1, both reliability measures exceeded the cutoff values of 0.70 (Fornell and Larcker 1981, Nunally 1978).

We assessed the convergent and discriminant validity of the reflective constructs using four methods: (1) the square root of the AVE of all constructs were much larger than all other cross-correlations; (2) all AVEs were well above 0.50, suggesting that the constructs captured much higher construct-related variance than error variance; (3) the correlations among all constructs were well below the 0.90 threshold, suggesting that all constructs were distinct from each other; and (4) all items loaded highest on their intended constructs, with all factor loadings greater than 0.70 (all t-values were significant).

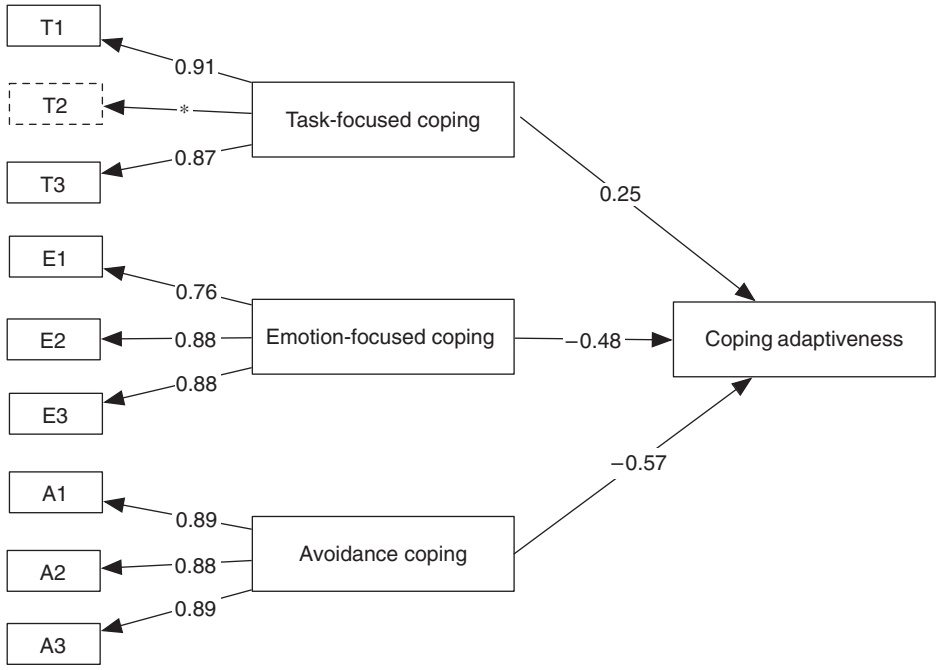
Both perceived threat and coping adaptiveness were modeled as second-order formative constructs. Perceived threat was modeled as a second-order formative construct with two first-order components: perceived susceptibility and perceived severity. The weights from the first-order components to the second-order constructs (0.85 and 0.43, respectively) have a t-statistic greater than 3.29. Coping adaptiveness (Figure 4) had three first-order components: task-focused coping, emotion-focused coping, and avoidance coping, with weights of 0.25, −0.48, and −0.57 respectively, all having t-statistics greater than 3.29. To test potential multicollinearity among the first constructs, we performed the variance inflation factor (VIF) test. The VIFs were well below 3.3, indicating that multicollinearity is not a cause of concern for either construct (Petter et al. 2007).

4.2. Testing the Structural Model

4.2.1. Control Variables. In testing our structural model, a number of control variables were entered in the PLS regression analysis for each of the following: phishing anxiety, coping adaptiveness, detection effort, and detection accuracy. Table 3 lists the relationships between the control variables and the constructs. Three task characteristic variables—familiarity with the business entity, the feeling of seeing an email before, and easiness of recognizing the emails—were irrelevant to phishing anxiety and were not linked to the latter.

As we can see from Table 3, females are more likely to engage in coping responses that are adaptive in nature and have higher accuracy. Education increases adaptive coping and enhances detection effort. Prior victimization (i.e., experience of identity theft) increases coping adaptiveness. Individuals with more Internet

Figure 4. Measurement of Coping Adaptiveness



*t-statistic (two-tailed) < 1.64.

experience are more likely to have adaptive coping responses. Number of daily emails and number of credit cards do not significantly impact any variables. Age increases coping adaptiveness, suggesting that older people are more engaged in adaptive coping responses than younger people, consistent with prior studies in phishing (Jagatic et al. 2007, Sheng et al. 2010, Wang et al. 2012, Workman 2008). Dispositional optimism decreases phishing anxiety and increases coping adaptiveness, suggesting that optimistic individuals are less anxious about phishing attacks and more engaged in adaptive coping responses. For the task characteristics, familiarity with the business entity increases accuracy. The feeling about having seen emails earlier ("Seen before" in Table 3) reduces detection accuracy. Easiness of an email set is positively related to detection accuracy, as one would expect.

Table 3. Effects of Control Variables

Control variables	Phishing anxiety	Coping adaptiveness	Detection effort	Detection accuracy
Gender (female)	0.06	0.14***	0.04	0.10**
Education	−0.04	0.08*	0.08*	−0.04
Prior victimization	0.05	0.16***	0.04	0.03
Income	−0.03	−0.07	0.01	0.08
Internet experience	0.08	0.14**	−0.05	−0.07
No. of daily emails	0.06	0.04	−0.02	0.03
No. of credit cards	0.00	−0.06	−0.05	−0.03
Age	0.00	0.09*	0.02	0.00
Disp. optimism	−0.16***	0.21***	−0.02	−0.10**
Business familiarity	—	0.06	−0.02	0.09*
Seen before	—	−0.07	−0.00	−0.09*
Task easiness	—	0.00	0.02	0.20***

*t-statistic (two-tailed) > 1.96; **t-statistic > 2.57; ***t-statistic > 3.29.

4.2.2. Hypothesis Testing. The PLS path coefficients of the research model are presented in Figure 5. The model explained 28% variance in detection accuracy. For clarity of presentation, the figure does not include those control variables whose effects are presented in Table 3. The total effects of the independent variables on the dependent variables are summarized in Table 4. The total effect is the sum of the direct and indirect effects of an independent variable on the dependent variable in the model. Perceived threat ($\beta = -0.15$, $p < 0.001$) has a significant negative impact, while perceived detection efficacy ($\beta = 0.09$, $p < 0.05$) has a significant positive impact, on coping adaptiveness, supporting H1 and H2, respectively. For H1, particularly, we argue in Section 2.2.1 that a perceived threat of phishing attacks increases task-focused coping, emotion-focused coping, and avoidance coping, although the net effect is decreased coping adaptiveness. This is confirmed by the data: as Table D1 in Online Appendix D shows, perceived severity has a positive correlation ($r = 0.27$, $p < 0.01$) with task-focused coping, and perceived susceptibility has a positive correlation with emotion-focused coping ($r = 0.33$, $p < 0.01$) and with avoidance coping ($r = 0.38$, $p < 0.01$), thus providing support to our argument. Table D1 also shows that detection efficacy is positively correlated with task-focused coping ($r = 0.25$, $p < 0.01$) and negatively correlated with emotion-focused coping

($r = -0.23$, $p < 0.01$) and avoidance coping ($r = -0.10$, $p < 0.05$), providing support to our rationale in H2.

Meanwhile, a perceived threat negatively influences perceived phishing detection efficacy ($\beta = -0.18$, $p < 0.01$), supporting H3. Perceived threat ($\beta = 0.42$, $p < 0.001$) positively influences, while perceived detection efficacy ($\beta = -0.10$, $p < 0.01$) negatively impacts, phishing anxiety, validating H4 and H5, respectively. Our results also indicate phishing anxiety decreases the adaptiveness of coping responses in phishing detection ($\beta = -0.18$, $p < 0.001$); thus, H6 is supported. Particularly, Table D1 in Online Appendix D shows that phishing anxiety is positively correlated with emotion-focused coping ($r = 0.34$, $p < 0.01$) and avoidance coping ($r = 0.24$, $p < 0.01$), but has no correlation with task-focused coping ($r = 0.01$, $p > 0.1$), thus validating our rationale in H6. Further analysis shows that without the presence of phishing anxiety in the model, the effect of a perceived threat is -0.23, and that of perceived detection efficacy is 0.11. A Sobel test (MacKinnon et al. 1995) indicates the effect of perceived threat is partially mediated by phishing anxiety (with a p-value less than 0.001).

Our results also suggest that coping adaptiveness positively affects detection effort ($\beta = 0.28$, $p < 0.001$) and detection accuracy ($\beta = 0.22$, $p < 0.001$), supporting H7 and H8. Further examinations of the correlations in Table D1 provide additional evidence, that task-focused coping is positively correlated with detection effort ($r = 0.10$, $p < 0.05$) and accuracy ($r = 0.15$, $p < 0.01$), while emotion-focused coping and avoidance coping are negatively correlated with effort ($r = -0.19$, $p < 0.01$ and $r = -0.31$, $p = 0.01$, respectively) and accuracy ($r = -0.26$, $p < 0.01$ and $r = -0.27$, $p = 0.01$, respectively). Detection effort has a significant effect on decision accuracy ($\beta = 0.33$, $p < 0.001$), validating H9. In the absence of detection effort, the effect of coping adaptiveness on decision accuracy increases ($\beta = 0.28$, $p < 0.001$). A Sobel test indicates the mediating effect of the detection effort is significant, with a p-value less than 0.001. As the effect of coping adaptiveness on decision accuracy remains significant with the presence of detection effort, it can be concluded that detection effort partially mediates the effect of coping adaptiveness on decision accuracy in phishing detection.

Table 4. Total Effect of the Independent Variables on the Dependent Variables

	Phishing anxiety	Coping adaptiveness	Detection effort	Detection accuracy
Perceived threat	0.44***	−0.24***	−0.07***	−0.08***
Detection efficacy	−0.10*	0.11*	0.03*	0.03*
Phishing anxiety	—	−0.18***	−0.05***	−0.06***
Coping adaptiveness	—	—	0.28***	0.31***
Decision effort	—	—	—	0.33***

*t-statistic > 1.96; ***t-statistic > 3.29.

Table 5. Total Effect of the Independent Variables on the Dependent Variables: Legitimate Emails

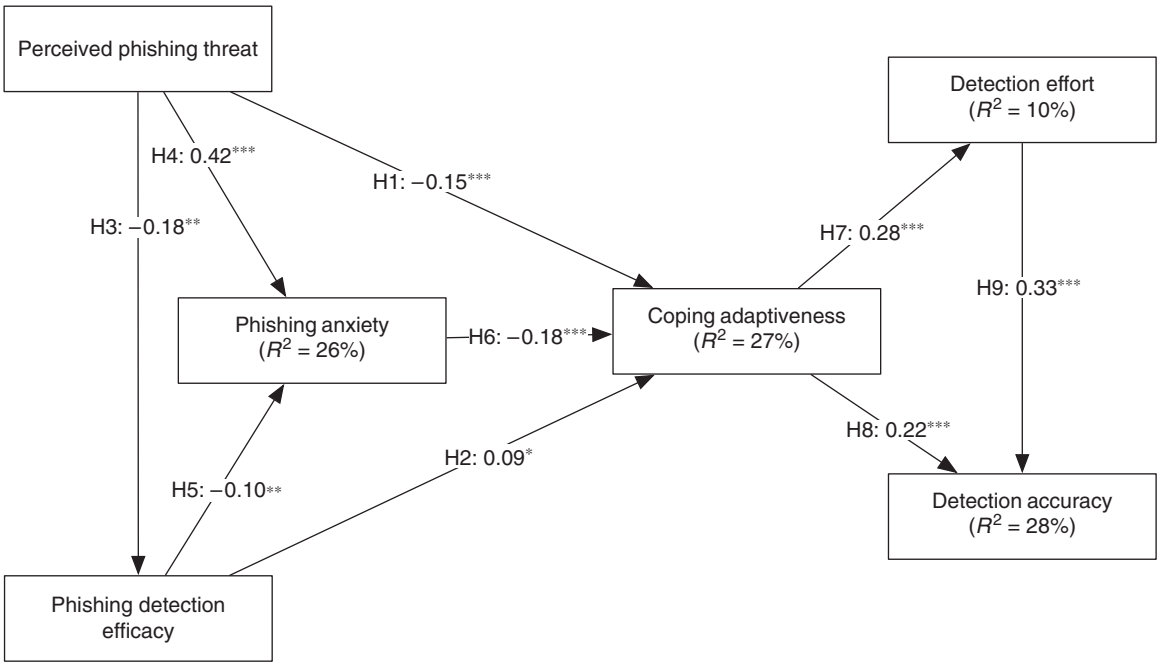
	Phishing anxiety	Coping adaptiveness	Detection effort	Detection accuracy
Perceived threat	0.44***	−0.24***	−0.09***	−0.04**
Detection efficacy	−0.10*	0.11*	0.04*	0.02†
Phishing anxiety	—	−0.18***	−0.07***	−0.03**
Coping adaptiveness	—	—	0.37***	0.16***
Detection effort	—	—	—	0.28***

*t-statistic > 1.96; **t-statistic > 2.57; ***t-statistic > 3.29; †t-statistic > 1.64.

To test H10, we first split the emails that an individual judged into two subsets, one with legitimate emails and the other with phishing emails. Detection effort and accuracy were then calculated for each subset. The research model was then reestimated based on the newly calculated detection effort and accuracy. The results of the path models are presented in Figure 6 (judgments of legitimate emails) and Figure 7 (judgments of phishing emails), and the total effects of independent variables on dependent variables are summarized in Table 5 (judgments of legitimate emails) and Table 6 (judgments of phishing emails). The results show distinctions with regard to H8 (coping adaptiveness to detection accuracy) and H9 (detection effort to detection accuracy). In judging legitimate emails, the detection effort fully mediates the effect of coping adaptiveness on detection accuracy (or, conversely, false positive rate). Coping adaptiveness does not have a significant impact on detection accuracy ($\beta = 0.05$, $p > 0.10$) with the presence of detection effort (which significantly increases detection accuracy ($\beta = 0.28$, $p < 0.001$); Figure 5). Yet the total effect of coping adaptiveness on accuracy, 0.16 (see Table 5), is significant ($p < 0.001$). In judging phishing emails, detection effort does not have a significant impact on accuracy (or, conversely, false negative rate; $\beta = 0.03$, $p > 0.10$) but coping adaptiveness has an impact ($\beta = 0.22$, $p < 0.001$). Therefore, H10 is supported. Our data also show that detection accuracy related to legitimate emails is 59% (or the false positive rate is 41%), while that related to phishing emails is 75% (or the false negative rate is 25%), suggesting the existence of lie bias in phishing detection. Further detection effort is better explained by coping adaptiveness in judging legitimate emails than in judging phishing emails. These validate our rationale in H10.

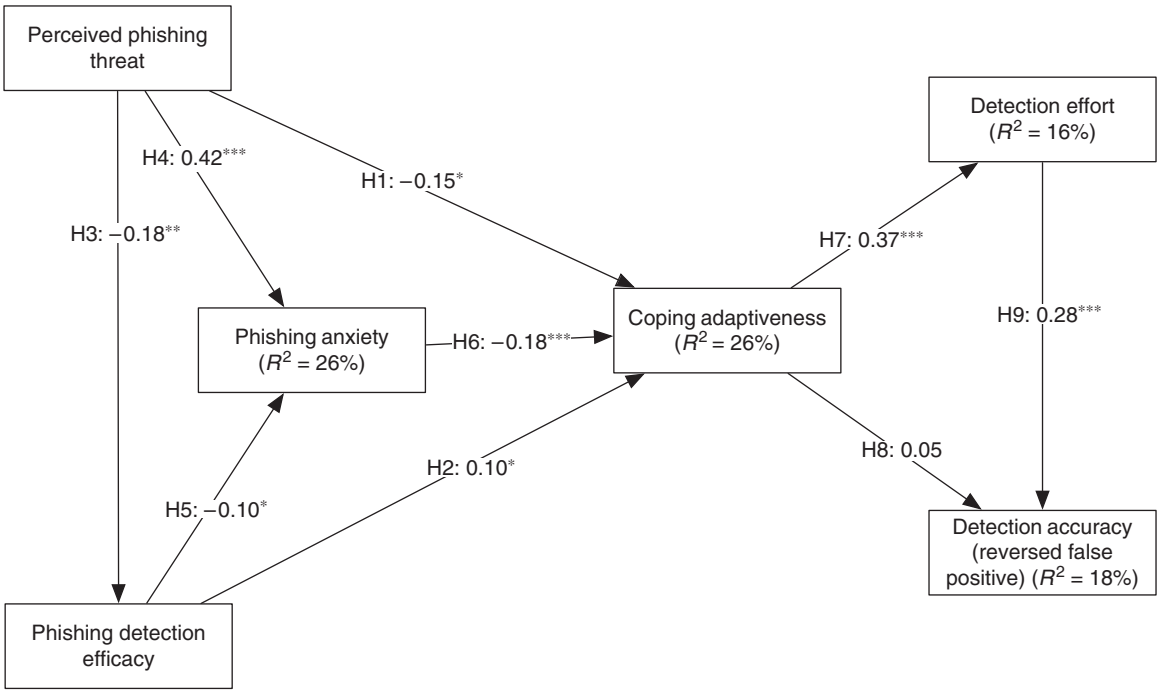
4.2.3. Post Hoc Analysis. As we discussed earlier, users engage in a mix of coping responses in the process of phishing detection, and it is unclear how much adopted coping responses differ. To gain more insight, we performed a cluster analysis using a two-step approach in which subjects were grouped based on their scores of the three dimensions of coping.

Figure 5. Estimated Path Coefficients



*t-statistic > 1.96; **t-statistic > 2.57; ***t-statistic > 3.29.

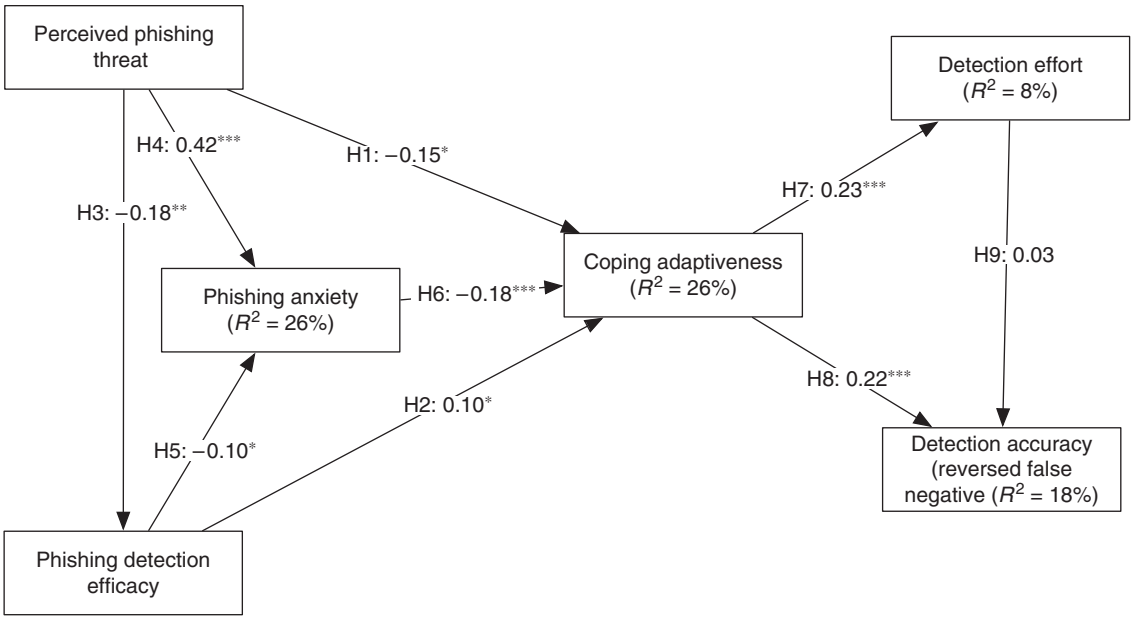
Figure 6. Judgments of Legitimate Emails



*t-statistic > 1.96; **t-statistic > 2.57; ***t-statistic > 3.29.

Two clusters were obtained. Table 7 summarizes the descriptive statistics of each cluster. As we can see, individuals in the first cluster (named *adapters*) adopt more task-focused coping and less emotion-focused and avoidance coping. By contrast, individuals in the second cluster (named *maladapters*) adopt less task-focused coping and more emotion-focused and avoidance coping; yet still, task-focused coping is more preferred in this group of subjects. Analysis of variance (ANOVA) tests indicate that the differences of the two

Figure 7. Judgments of Phishing Emails



*t-statistic > 1.96; **t-statistic > 2.57; ***t-statistic > 3.29.

Table 6. Total Effect of the Independent Variables on the Dependent Variables: Phishing Emails

	Phishing anxiety	Coping adaptiveness	Detection effort	Detection accuracy
Perceived threat	0.44***	−0.24***	−0.06***	−0.05***
Detection efficacy	−0.10*	0.11*	0.03*	0.03*
Phishing anxiety	—	−0.18***	−0.04**	−0.04***
Coping adaptiveness	—	—	0.23***	0.22***
Detection effort	—	—	—	0.03

*t-statistic > 1.96; **t-statistic > 2.57; ***t-statistic > 3.29.

clusters in task-focused coping, emotion-focused coping, and avoidance coping are all significant at 0.001.

Table 8 presents descriptive statistics of the principle constructs of the two clusters. Cluster 1 has a lower perceived threat, higher detection efficacy, and lower phishing anxiety than Cluster 2 (significant at 0.001 with ANOVA tests). The results are consistent with H1, H2, and H6. We also found that Cluster 1 has a higher detection effort and detection accuracy (significant at 0.001 with an ANOVA test), in line with H7 and H8.

Table 7. Cluster Analysis Results

Cluster	Task-focused coping	Emotion-focused coping	Avoidance coping
1: Adapters			
Mean	4.55	1.83	1.17
N	216	216	216
Std. deviation	0.49	0.71	0.30
2: Maladapters			
Mean	3.81	3.04	2.30
N	331	331	331
Std. deviation	0.68	0.79	0.81

Table 8. Descriptive Statistics of the Principle Constructs of the Two Clusters

Cluster	Perceived threat	Detection efficacy	Phishing anxiety	Detection effort	Detection accuracy
1: Adapters					
Mean	2.94	3.87	2.67	1.40	71.24
Std. deviation	0.66	0.79	1.02	0.39	14.50
2: Maladapters					
Mean	3.14	3.46	3.02	1.25	64.24
Std. deviation	0.72	0.84	0.93	0.49	15.29

5. Discussion and Conclusion

This study investigated the roles of coping responses in phishing email detection. We recognized three coping responses (task-focused coping, emotion-focused coping, and avoidance coping) and suggested a higher-order construct of coping adaptiveness consisting of these three components. We showed that coping adaptiveness was driven by perceived threat, perceived detection efficacy, and phishing anxiety, which in turn determined detection effort and detection accuracy. The study threw light into the black box of individuals' cognitive and behavioral responses in managing the demand of phishing detection.

5.1. Theoretical Contributions

The contributions of the study are threefold. First, a majority of the studies in the area of phishing susceptibility (see Online Appendix A for a review) have

focused on the effect of information cues such as design features and persuasive tactics of phishing emails in exploring user vulnerability and developing training programs. Yet research untangling how well users manage the detection of phishing has been sparse. This study extended the concept of coping to understand users' detection of phishing emails, enabling us to zoom in on the cognitive and behavioral processes at the point of detection. As shown in our results, coping plays an essential role in successfully differentiating legitimate business emails from phishing ones. Furthermore, our results suggest that coping and cognitive effort show different effects on false positives than on false negatives, two aspects that have never been explored and compared in the same theoretical framework. In addition, we have argued that users' propensity for bias, i.e., lie bias or truth bias, could be essential in understanding and mitigating the false positives and false negatives.

Second, we conceptualized coping adaptiveness by introducing both adaptive and maladaptive responses into the construct. Most studies on information security behavior (see Appendix A in Boss et al. 2015) have primarily conceptualized coping responses as one's attitude, intention, or behavior of taking a desired action, which is adaptive in nature. In this study, we found users not only form adaptive responses (such as task-focused coping) but also maladaptive responses (such as emotion-focused and avoidance coping) to information security threats. Coping is a complex process where individuals may engage in different responses (adaptive or maladaptive in nature) influencing their information security well-being and outcomes. The conceptualization enriches the theoretical and conceptual understanding of coping in the information security literature. Furthermore, by incorporating the second-order construct of coping adaptiveness into the research model, this study extended the EPPM, which traditionally treated danger control and fear control as dichotomous processes. Our results suggest individuals engage in a mix of coping responses in phishing detection. The model provides a parsimonious application of the EPPM to a new domain.

Third, in response to recent calls to better understand the role of negative emotional arousal (such as fear or anxiety) in the context of information security (Boss et al. 2015, Crossler et al. 2013), we incorporated phishing anxiety in our model following the EPPM. We found it has a negative direct effect on coping adaptiveness, and partially mediates the effect between perceived threat and coping adaptiveness. While prior research in information security (Boss et al. 2015) has argued for the positive impact of negative emotional arousal (such as fear or anxiety) on protective motivation, our study shows that it could be a double-edged sword that may increase maladaptive responses as well.

5.2. Practical Implications

Our study also has practical implications for phishing training. The first implication deals with the central role of coping adaptiveness in the behavioral response to phishing attacks. Prior studies in phishing training have primarily focused on a cognitive approach, training employees to recognize the information cues in phishing emails or websites (Kumaraguru et al. 2010, Sheng et al. 2007). However, it may not suffice to improve their detection outcomes since they may ignore the information cues in action (Dhamija et al. 2006). Our study suggests that it would be important, during the training, to bolster employees' coping skills, especially for the maladapters (Cluster 2 in Tables 7 and 8). For example, positive thinking and proper problem-solving strategies that can be related to phishing detection might be emphasized in such training to improve coping adaptiveness. More importantly, employees should be made aware of the ineffectiveness of emotion-focused coping and avoidance coping and learn to better monitor and self-regulate their psychological processes, so that they may devote sufficient effort to phishing detection.

The second implication deals with the negative role of phishing anxiety in phishing detection. One note of caution in phishing training is that such training may alter individuals' threat appraisal in regard to phishing attacks and unnecessarily boost phishing anxiety. This has been evidenced in prior studies suggesting that phishing training makes individuals more suspicious (Anandpara et al. 2007, Kumaraguru et al. 2010). Although this may, in fact, alert people about phishing attacks, such training should be crafted to not provoke too much phishing anxiety, as excessively heightened and intensified anxiety may backfire and reduce adaptive coping in dealing with security threats (Liang and Xue 2009). Prior studies have also suggested that fear appeals may induce lie bias in phishing detection (Anandpara et al. 2007, Kumaraguru et al. 2010). Such a bias may increase a user's false positive rate, as their tendency to misjudge nonthreats as threats can be increased. Therefore, training should avoid exaggerating user vulnerability and consequences of victimization, and avoid heightening and intensifying phishing anxiety. Furthermore, the training programs should be aware of whether the material will lead users to be lie biased or truth biased, and correspondingly reduce both false positives and false negatives.

The last implication deals with the distinct roles of detection effort in judging legitimate emails and phishing emails. As illustrated above, the detection effort fully mediates the impact of coping adaptiveness on detection accuracy for legitimate emails, but it has no effect on detection accuracy for phishing emails. This suggests the difficulty or uncertainty in detecting phishing emails, as spending additional time on

an email may not be sufficient to help detect phish emails. We suggest that it is not the total amount of time that can help a person to detect phish emails, but how the person effectively uses the time: for example, what visceral triggers and phishing deception indicators does the person attend to (Wang et al. 2012)? This also justifies offering systematic training to employees rather than simply sending them notifications of potential phishing threats (Kumaraguru et al. 2010).

5.3. Limitations and Future Studies

There are several limitations to the study that warrant consideration. First, one potential limitation, which is common to all lab studies in deception, is that being a subject primes suspicion, and truth bias may be reduced (Levine 2014). In the scenario of phishing detection, the situations that provoke users' truth bias or lie bias need to be further explored, and the behavioral differences of users with the two different types of biases compared. Furthermore, the results in this study should be interpreted within certain boundaries. In our study, the subjects were reminded about phishing attacks and made aware that some of the emails they would judge could be phishing emails. Translated to real life, the findings may be better applicable to those who are consciously aware of the threat of phishing attacks in their daily email processing, satisfying the fear-appeal assumptions of the EPPM (Witte 1992). The findings, however, may not apply to those who have no knowledge of or have not been communicated with regarding the risks of phishing attacks. Neither may the findings be applicable to those who believe that legislative and technological solutions will guarantee the blocking of all phishing emails and thus consider phishing detection irrelevant to them. For those subjects, effective communication of phishing threats would be necessary to engage them in active detection of phishing emails, which this study attempted to address.

Second, in the survey experiment, each respondent was asked to indicate whether an email was legitimate or not. The term "legitimate" is commonly used to refer to genuine business emails and appeared frequently in empirical research on phishing detection (Dhamija et al. 2006, Downs et al. 2006, Kumaraguru et al. 2010, Sheng et al. 2010, Wright and Marett 2010). However, some people may interpret legitimate emails as solicited business emails only, but not unsolicited emails sent from authentic business entities. In the current study, we did not have a manipulation check on the respondents' understanding of this term. However, we do not think the possible misinterpretation of the concept threatens the validity of our study, given the design of the research procedure and the outcomes. First, the consent form and the instructions (see Online Appendix B) highlighted the distinction between phishing emails and legitimate emails, and the respondents had to acknowledge the consent form to move on. Second, before judging the emails, the respondents answered a set of questions reflecting their threat and coping appraisal with items related to phishing (see Step 2 in Figure 3 and also Online Appendix C), further seating them in the context. Third, we compared our detection accuracy measure with that in the peer literature (see Online Appendix E): as shown in Table E1, detection accuracy reported in prior literature ranges between 42% and 79%, with ours being 67%. The result did not deviate from prior findings. In addition, we did a Google search for the term "legitimate email." All of the responses in the first three pages to the search that came up telling how to recognize legitimate emails from phishing emails, or how to verify the source of the email if it is legitimate or not, were consistent with the interpretation that we used in the paper, thus suggesting that the path we took also matches the understanding that most of the respondents have. Thus, we conclude that on the overall the judgments of respondents in our study were valid.

The third limitation is that, as subjects were explicitly requested to differentiate among legitimate and phishing emails, we did not operationalize the perceived response efficacy of the respondents. This can be incorporated into the model in the future, for situations where users may engage in coping responses in areas other than to maximize the probability of detection, perhaps, for example, to enhance the efficiency of email processing. Fourth, our current study focused on an individual's efficacy in detecting phishing. With the development of antiphishing technologies such as visual email authentication and identification services (Herath et al. 2012, Wang et al. 2009), future studies could further investigate how technology assistance changes one's coping with respect to phishing attacks. Finally, we used detection accuracy as the dependent variable, although an individual's confidence on her decision may also affect the possibility for her to become a victim of phishing emails. Therefore, the relationship between confidence, accuracy, and subsequent protective behavior regarding phishing attacks can be further explored.

Acknowledgments

The authors thank the senior editor, the associate editor, and the anonymous referees for their critical comments that greatly improved this paper. The usual disclaimer applies.

References

Albrechtsen JS, Meissner CA, Susa KJ (2009) Can intuition improve deception detection performance? *J. Experiment. Soc. Psych.* 45(4):1052–1055.

Anandarajan M, Paravastu N, Arinze B, D'Ovdio R (2012) Online identity theft: A longitudinal study of individual threat-response and coping behaviors. *J. Inform. System Security* 8(2): 43–69.

Anandpara V, Dingman A, Jakobsson M, Liu D (2007) Phishing IQ tests measure fear, not ability. Dietrich S, Dhamija R, eds. *Proc. 11th Internat. Conf. Financial Cryptography and 1st Internat. Conf. Usable Security* (Springer-Verlag, Berlin Heidelberg), 362–366.

Anderson CL, Agarwal R (2010) Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quart.* 34(3):613–643.

APWG (2010) Consumer advice: How to avoid phishing scams. Anti-Phishing Working Group. http://www.antiphishing.org/resources/overview/avoid-phishing-scams.

APWG (2014) Phishing activity trends report, 1st Quarter 2014. https://docs.apwg.org/reports/apwg_trends_report_q1_2014.pdf.

Arkers HR (1991) Costs and benefits of judgment errors: Implications for debiasing. *Psych. Bull.* 110(3):486–498.

Bandura A (1982) Self-efficacy mechanism in human agency. *Amer. Psych.* 37(2):122–147.

Beaudry A, Pinsonneault A (2010) The other side of acceptance: Studying the direct and indirect effects of emotions on information technology use. *MIS Quart.* 34(4):689–710.

Bettman JJ, Johnson EJ, Payne JW (1990) A componential analysis of cognitive effort in choice. *Organ. Behav. Human Decision Processes* 45(1):111–139.

Boss SR, Galletta DF, Lowry PB, Moody GD, Polak P (2015) What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quart.* 39(4):837–864.

Caputo DD, Pfleeger SL, Freeman JD, Johnson ME (2014) Going spear phishing: Exploring embedded training and awareness. *IEEE Security Privacy* 12(1):2–12.

Champion VL, Skinner CS, Menon U (2004) A breast cancer fear scale: psychometric development. *J. Health Psych.* 9(6):753–762.

Chen R, Wang J, Herath T, Rao HR (2011) An investigation of email processing from a risky decision making perspective. *Decision Support Systems* 52(1):73–81.

Churchill GA Jr (1979) A paradigm for developing better measures of marketing constructs. *J. Marketing Res.* 16(1):64–73.

Compeau DR, Higgins CA (1995) Computer self-efficacy: Development of a measure and initial test. *MIS Quart.* 19(2):189–211.

Cranor LF (2008) A framework for reasoning about the human in the loop. Churchill E, Dhamija R, eds. *Proc. 1st Conf. Usability, Psych., Security* (USENIX Association, Berkeley, CA).

Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R (2013) Future directions for behavioral information security research. *Comput. Security* 32(1):90–101.

Dhamija R, Tygar JD, Hearst M (2006) Why phishing works. Grinter R, Rodden T, Aoki P, Cutrell E, Jeffries R, Olson G, eds. *SIGCHI Conf.* (ACM, New York), 581–590.

Dodge RC Jr, Carver C, Ferguson AJ (2007) Phishing for user security awareness. *Comput. Security* 26(1):73–80.

Downs JS, Holbrook MB, Cranor LF (2006) Decision strategies and susceptibility to phishing. Cranor LF, ed. *Proc. Second Sympos. Usable Privacy Security* (ACM, New York), 79–90.

Downs JS, Holbrook M, Cranor LF (2007) Behavioral response to phishing risk. *Proc. Anti-Phishing Working Groups 2007 eCrime Researchers Summit, Pittsburgh*, 37–44.

El-Din RS, Cairns P, Clark J (2014) Mobile users' strategies for managing phishing attacks. *J. Management Strategy* 5(2):70–81.

Endler NS, Parker JDA (1990) Multidimensional assessment of coping: A critical evaluation. *J. Personality Soc. Psych.* 58(5):844–854.

Floyd DL, Prentice-Dunn S, Rogers RW (2000) A meta-analysis of research on protection motivation theory. *J. Appl. Soc. Psych.* 30(2):407–429.

Fornell C, Larcker DF (1981) Evaluating structural equation models with unobservable variables and measurement error. *J. Marketing Res.* 18(1):39–50.

Furnell S (2007) Phishing: Can we spot the signs? *Comput. Fraud Security* 2007(3):10–15.

Garbarino EC, Edell JA (1997) Cognitive effort, affect, and choice. *J. Consumer Res.* 24(2):147–158.

Gefen D, Rigdon EE, Straub D (2011) An update and extension to SEM guidelines for administrative and social science research. *MIS Quart.* 35(2):iii–xiv.

Gupta S, Kumaraguru P (2014) Emerging phishing trends and effectiveness of the anti-phishing landing page. https://arxiv.org/pdf/1406.3682.

Hann IH, Hui KL, Lee SYT, Png IPL (2007) Overcoming online information privacy concerns: An information-processing theory approach. *J. Management Inform. Systems* 24(2):13–42.

Hee S, Levine T (2010) A probability model of accuracy in deception detection experiments. *Comm. Monographs* 68(2):201–210.

Herath T, Chen R, Wang J, Banjara K, Wilbur J, Rao HR (2012) Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Inform. Systems J.* 24(1):61–84.

Hong J (2012) The state of phishing attacks. *Comm. ACM* 55(1):74–81.

Jagatic TN, Johnson NA, Jakobsson M, Menczer F (2007) Social phishing. *Comm. ACM* 50(10):94–100.

Jakobsson M, Myers S, eds. (2006) *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft* (Wiley, Hoboken, NJ).

Johnson EJ, Payne JW (1985) Effort and accuracy in choice. *Management Sci.* 31(4):395–414.

Johnston AC, Warkentin M (2010) Fear appeals and information security behaviors: An empirical study. *MIS Quart.* 34(3):549–566.

Johnston AC, Warkentin M, Siponen M (2015) An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quart.* 39(1):113–134.

Kumaraguru P (2009) PhishGuru: A system for educating users about semantic attacks. Doctoral dissertation, Carnegie Mellon University, Pittsburgh.

Kumaraguru P, Sheng S, Acquisti A (2008) Lessons from a real world evaluation of anti-phishing training. *Proc. Anti-Phishing Working Groups 2008 eCrime Researchers Summit, Atlanta*.

Kumaraguru P, Sheng S, Acquisti A, Cranor LF, Hong J (2010) Teaching Johnny not to fall for phish. *ACM Trans. Internet Tech.* 10(2):1–31.

Lai F, Li D, Hsieh C-T (2012) Fighting identity theft: The coping perspective. *Decision Support Systems* 52(2):353–363.

Lazarus RS, Folkman S (1984) *Stress, Appraisal, and Coping* (Springer, New York).

Lee KJ, Song IY (2007) Investigating information structure of phishing emails based on persuasive communication perspective. *J. Digital Forensics, Security Law* 2(3):29–44.

Lerner JS, Tetlock PE (2003) Bridging individual, interpersonal, and institutional approaches to judgment and decision making: The impact of accountability on cognitive bias. Schneider SL, Shanteau J, eds. *Emerging Perspectives on Judgment and Decision Research* (Cambridge University Press, New York), 431–457.

Levine TR, ed. (2014) *Encyclopedia of Deception* (Sage, Thousand Oaks, CA).

Levine TR, Kim RK, Park HS, Hughes M (2006) Deception detection accuracy is a predictable linear function of message veracity base-rate: A formal test of Park and Levine's probability model. *Comm. Monographs* 73(3):243–260.

Liang H, Xue Y (2009) Avoidance of information technology threats: A theoretical perspective. *MIS Quart.* 33(1):71–90.

Liang H, Xue Y (2010) Understanding security behaviors in personal computer usage: A threat avoidance perspective. *J. Assoc. Inform. Systems* 11(7):394–413.

Liu G, Xiang G, Pendleton BA, Hong JI, Liu W (2011) Smartening the crowds: Computational techniques for improving human verification to fight phishing scams. Cranor LF, ed. *Proc. 7th Sympos. Usable Privacy Security* (ACM, New York), Article 8.

Luo XR, Zhang W, Burd S, Seazzu A (2013) Investigating phishing victimization with the heuristic-systematic model: A theoretical framework and an exploration. *Comput. Security* 38(1):28–38.

MacKinnon DP, Warsi G, Dwyer JH (1995) A simulation study of mediated effect measures. *Multivariate Behav. Res.* 30(1):41–62.

Masip J, Alonso H, Garrido E, Anton C (2005) Generalized communicative suspicion (GCS) among police officers: Accounting for the investigator bias effect. *J. Appl. Soc. Psych.* 35(5):1046–1066.

Matthews G, Campbell SE (1998) Task-induced stress and individual differences in coping. *Proc. Human Factors Ergonomics Soc. 42nd Annual Meeting*, Vol. 42(11) (Sage, Thousand Oaks, CA), 821–825.

Matthews G, Hillyard EJ, Campbell SE (1999) Metacognition and maladaptive coping as components of test anxiety. *Clinical Psych. Psychotherapy* 6(2):111–125.

Matthews G, Zeidner M, Roberts RD (2007) *Emotional Intelligence: Science and Myth* (MIT Press, Cambridge, MA).

Matthews G, Warm JS, Reinerman LE, Langheim LK, Saxby DJ (2010) Task engagement, attention, and executive control. Gruszka A, Matthews G, Szymura B, eds. *Handbook of Individual Differences in Cognition: Attention, Memory, and Executive Control* (Springer, New York), 205–230.

Matthews G, Emo AK, Funke G, Zeidner M, Roberts RD, Costa PTJ, Schulze R (2006) Emotional intelligence, personality, and task-induced stress. *J. Experiment. Psych.: Appl.* 12(2):96–107.

Matthews G, Campbell SE, Falconer S, Joyner LA, Huggins J, Gilliland K, Grier R, Warm JS (2002) Fundamental dimensions of subjective state in performance settings: Task engagement, distress, and worry. *Emotion* 2(4):315–340.

Microsoft (2010) How to recognize phishing e-mails or links. https://www.microsoft.com/en-us/safety/online-privacy/phishing-symptoms.aspx.

Mohebzada JG, Zarka AE, Bhojani AH, Darwish A (2012) Phishing in a university community: Two large scale phishing experiments. 2012 *Internat. Conf. Innovations Inform. Tech., Abu Dhabi, Al-Ain, UAE*, 249–254.

Moody G, Galletta DF, Walker J, Dunn BK (2011) Which phish get caught? An exploratory study of individual susceptibility to phishing. *Internat. Conf. Inform. Systems*.

Nunally JC (1978) *Psychometric Theory* (McGraw-Hill, New York).

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

Payne JW (1982) Contingent decision behavior. *Psych. Bull.* 92(2): 382–402.

Petter S, Straub D, Rai A (2007) Specifying formative constructs in information systems research. *MIS Quart.* 31(4):623–656.

Piquero NL, Cohen MA, Piquero AR (2011) How much is the public willing to pay to be protected from identity theft? *Justice Quarterly* 28(3):437–459.

Popova L (2012) The extended parallel process model: Illuminating the gaps in research. *Health Ed. Behav.* 39(4):455–473.

Public Safety Canada (2009) Phishing: A new form of identity theft. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-phshng/index-en.aspx.

Ringle CM, Wende S, Will S (2005) SmartPLS 2.0 (M3) beta. SmartPLS, Hamburg, Germany.

Rippetoe PA, Rogers RW (1987) Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *J. Personality Soc. Psych.* 52(3):596–604.

Rogers RW (1975) A protection motivation theory of fear appeals and attitude change. *J. Psych.* 91(1):93–114.

RSA (2012) Phishing and the social world. https://www.emc.com/collateral/fraud-report/online-fraud-report-1012.pdf.

Scheier MF, Carver CS, Bridges MW (1994) Distinguishing optimism from neuroticism (and trait anxiety, self-mastery, and self-esteem): A reevaluation of the life 39 orientation test. *J. Personality Soc. Psych.* 67(6):1063–1078.

Shaw TH, Matthews G, Warm JS, Finomore VS, Silverman L, Costa PT Jr (2010) Individual differences in vigilance: Personality, ability and states of stress. *J. Res. Personality* 44(3):297–308.

Sheng S (2009) A policy analysis of phishing countermeasures. Doctoral dissertation, Carnegie Mellon University, Pittsburgh.

Sheng S, Holbrook M, Kumaraguru P, Cranor LF, Downs J (2010) Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. Mynatt E, ed. *Proc. 28th Internat. Conf. Human Factors Comput. Systems* (ACM, New York), 1–10.

Sheng S, Magnien B, Kumaraguru P, Acquisti A, Cranor LF, Hong J, Nunge E (2007) Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. Cranor LF, ed. *Proc. 3rd Sympos. Usable Privacy Security* (*SOUPS 2007*), Vol. 229 (ACM, New York), 88–99.

Siegel-Jacobs K, Yates JF (1996) Effects of procedural and outcome accountability on judgment quality. *Organ. Behav. Human Decision Processes* 66:1–17.

Symantec (2014) Internet security threat report 2014. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

Todd P, Benbasat I (1999) Evaluating the impact of DSS, cognitive effort, and incentives on strategy selection. *Inform. Systems Res.* 10(4):356–374.

Todd P, Benbasat I (2000) Inducing compensatory information processing through decision aids that facilitate effort reduction: An experimental assessment. *J. Behav. Decision Making* 13(1):91–106.

Vinzi VE, Chin WW, Henseler J, Wang H (2010) *Handbook of Partial Least Squares* (Springer, New York).

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

Wang J, Chen R, Herath T, Rao HR (2009) Visual e-mail authentication and identification services: An investigation of the effects on e-mail use. *Decision Support Systems* 48:92–102.

Wang J, Herath T, Chen R, Vishwanath A, Rao HR (2012) Phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Trans. Professional Comm.* 55(4): 345–362.

Webster DM, Richter L, Kruglanski AW (1996) On leaping to conclusions when feeling tired: Mental fatigue effects on impressional primacy. *J. Experiment. Soc. Psych.* 52:181–195.

Wilfong JD (2006) Computer anxiety and anger: The impact of computer use, computer experience, and self-efficacy beliefs. *Comput. Human Behav.* 22:1001–1011.

Witte K (1992) Putting the fear back into fear appeals: The extended parallel process model. *Comm. Monographs* 59:329–349.

Witte K, Allen M (2000) A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Ed. Behav.* 27(5): 591–615.

Workman M (2008) Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *J. Amer. Soc. Inform. Sci. Tech.* 59(4):662–674.

Wright AJ (2010) The impact of perceived risk on risk-reducing behaviours. French D, Vedhara K, Kaptein AA, Weinman J, eds. *Health Psychology* (Blackwell, Oxford, UK), 111–121.

Wright RT, Marett K (2010) The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *J. Management Inform. Systems* 27(1):273–303.

Wright RT, Jensen ML, Thatcher JB, Dinger M, Marett K (2014) Influence techniques in phishing attacks: An examination of vulnerability and resistance. *Inform. Systems Res.* 25(2):385–400.

Zeidner M, Saklofske D (1996) Adaptive and maladaptive coping. Zeidner M, Endler NS, eds. *Handbook of Coping: Theory, Research, Applications* (Wiley, New York), 505–531.

Zhang L, McDowell WC (2009) Am I really at risk? Determinants of online users' intentions to use strong passwords. *J. Internet Commerce* 8(3–4):180–197.