Journal of the Association for Information Systems

Volume 16 | Issue 6 Article 2

6-20-2015

Fake-Website Detection Tools: Identifying Elements that Promote Individuals' Use and Enhance Their Performance

Fatemeh Mariam Zahedi
University of Wisconsin, zahedi@uwm.edu

Ahmed Abbasi
University of Virginia, abbasi@comm.virginia.edu

Yan Chen
Auburn University at Montgomery, ychen3@aum.edu

Recommended Citation
Zahedi, Fatemeh Mariam; Abbasi, Ahmed; and Chen, Yan (2015) "Fake-Website Detection Tools: Identifying Elements that Promote Individuals' Use and Enhance Their Performance," *Journal of the Association for Information Systems*, 16(6), .
DOI: 10.17705/1jais.00399
Available at: https://aisel.aisnet.org/jais/vol16/iss6/2

Journal of the Association for Information Systems
JAIS

Research Article

Fake-Website Detection Tools: Identifying Elements that Promote Individuals' Use and Enhance Their Performance

Fatemeh Mariam Zahedi
University of Wisconsin
zahedi@uwm.edu

Ahmed Abbasi
University of Virginia
abbasi@comm.virginia.edu

Yan Chen
Auburn University at Montgomery
ychen3@aum.edu

Abstract

By successfully exploiting human vulnerabilities, fake websites have emerged as a major source of online fraud. Fake websites continue to inflict exorbitant monetary losses and also have significant ramifications for online security. We explore the process by which salient performance-related elements could increase the reliance on protective tools and, thus, reduce the success rate of fake websites. We develop the theory of detection tool impact (DTI) for this investigation by borrowing and contextualizing the protection motivation theory. Based on the DTI theory, we conceptualize a model to investigate how salient performance and cost-related elements of detection tools could influence users' perceptions of the tools and threats, efficacy in dealing with threats, and reliance on such tools. The research method was a controlled lab experiment with a novel and extensive experimental design and protocol in two distinct domains: online pharmacies and banks. We found that the detector accuracy and speed, reflecting in response efficacy as perceived by users, form the pivotal coping mechanism in dealing with security threats and are major conduits for transforming salient performance-related elements into increased reliance on the detector. Furthermore, reported reliance on the detector showed a significant impact on the users' performance in terms of self-protection. Therefore, users' perceived response efficacy should be used as a critical metric to evaluate the design, assess the performance, and promote the use of fake-website detectors. We also found that cost of detector error had profound impacts on threat perceptions. We discuss the significant theoretical and empirical implications of the findings.

Keywords: *Protection Motivation Theory, Experimental Design, Spoofed Websites, Concocted Websites, Detection Tool, Protective IT Artifact.*

* Fiona Fui-Hoon Nah as the accepting senior editor. This article was submitted on 23rd February 2012 and went through three revisions.

Volume 16, Issue 6, pp. 448-484, June 2015

Fake-Website Detection Tools: Identifying Elements that Promote Individuals' Use and Enhance Their Performance

1. Introduction

One of the most vulnerable points in the online security process is when users decide to visit and use a website (Schneier, 2000). Semantic attacks focus on "targeting the people" instead of exploiting hardware and software vulnerabilities as done by many other Internet security attacks, such as viruses, denial of service, and malware (Schneier, 2000). In such attacks, users' unpredictable behaviors play a critical role (Cranor, 2008; Kumaraguru, Sheng, Aquisti, Cranor, & Hong, 2010). Fake websites take advantage of this weak point in the security loop by posing as legitimate providers of information, goods, and services. As such, they rely on meaningful content to exploit weaknesses in human recognition of such attacks (Schneier, 2000).

Fake websites generate billions of dollars in fraudulent revenue by exploiting such human vulnerabilities (Zhang, Egelman, Cranor, & Hong, 2007) and are estimated to comprise nearly 20 percent of the Web (Gyongyi & Garcia-Molina, 2005). Fake websites offering harmful anti-virus software have defrauded 43 million users (Willis, 2009). According to an FDA study, less than 10 percent of the 12,000 Internet pharmacies examined were legitimate (Krebs, 2005). Moreover, the problem has worldwide reach; recently, a group of fraudsters in China developed fake military hospital websites used to defraud over 10,000 people (An, 2010). A 2011 Gartner report notes that phishing attacks using fake websites remain one of the biggest forms of Internet fraud for individuals and organizations (Gartner, 2011). Even more damaging than the immediate monetary losses is the potential for identity theft, where the personal information is used to open additional accounts (McAfee, 2011b). Javelin Strategy (2014) has reported that more than 13 million people were the victim of identity theft in 2013. In such situations, the direct monetary losses account for only 10 percent of the total fraud cost, with remediation and reputation costs (e.g., impact on credit scores/ratings) encompassing the majority of the losses (Lennon, 2011).

Fake websites also have dire ramifications for Internet users' health and wellness. According to studies conducted by the World Health Organization and other organizations, numerous deaths have been attributed to fake medical websites, while the number of people visiting such sites continues to increase dramatically (Easton, 2007; Armin, 2010). Consequently, in addition to monetary losses, fake websites have negative long-term trust and security-related implications at the global level (Malhotra, Kim, & Agarwal, 2004).

Countering fake-website attacks requires warning and educating users (Kumaraguru, 2009; Kumaraguru et al., 2010). Fake-website detection tools are designed to warn users. Repeated use of detection tools could also increase users' confidence in their own abilities to spot and avoid attacks. Therefore, the effectiveness of such tools is predicated on their use (Wu, Miller, & Garfunkel, 2006). To this end, we use a user-centered approach to investigate the relations between critical tool elements and the actual reliance on fake-website detection tools.

Few studies have examined how performance-related elements and cost of error could influence users' security perceptions and reliance on protective IT artifacts. We define protective IT artifacts as a type of IT artifact that protects users from damages caused by malicious software and fake websites. This definition is similar to Dinev and Hu's (2007) but extended to explicitly include fake websites. Given the significance of fake websites in terms of the hefty monetary loss and social costs inflicted, such an extension is warranted (Dinev, 2006; Jagatic, Johnson, Jakobsson, & Menczer, 2007; Abbasi, Zhang, Zimbra, Chen, & Nunamaker, 2010; Xiao & Benbasat, 2011). Previous studies have investigated how users react to the interfaces of fake-website detection tools (Wu et al., 2006) and salient interface design elements for such tools (Chen, Zahedi, & Abbasi, 2011). Others have analyzed the effectiveness of a particular warning message, such as the SSL warning (Sunshine, Egelman, Almuhimedi, Atri, & Cranor, 2009) and new models or methods that assist with users' security-critical decision making process (Cranor, 2008). These studies have been exploratory for the most part and provide limited theoretical insights regarding individuals' reactions. To the best of our knowledge, this paper is among the first to investigate the salient elements related to detection tools' performance (benefit), cost of error, and context-sensitive factors (domain and threat types) that could

influence people's reliance on tools in protecting themselves against fake-website attacks. To do so, we pose the following specific research questions: do a tool's salient elements impact users' reliance on the tool and their self-protection performance? If so, what is the process by which such elements alter users' behaviors and self-protection performance? Do context-sensitive elements of detection tools influence the above process?

In formulating the conceptual model to address the research questions, we draw on the protection motivation theory (PMT) (Rogers, 1975; Rogers, 1983) and extend the theory by contextualizing it to include context-specific factors salient to fake-website detection tools' performance and users' self-protection performance. A novel experimental design, with extensive stimuli development using carefully identified fake websites, guided the data collection for this study.

This paper makes important and novel theoretical and empirical contributions. Our research uncovers the process by which the salient elements of fake-website detection tools influence users' coping appraisals, alter their threat perceptions, and impact their reliance on the tool and self-protection performance. We extend protection motivation theory (PMT) to contextualize it to account for the context-specificity of the salient tool elements and users' reliance and performance as well as for the context-sensitivity of domains and threat types. Based on this theoretical framework, our work shows how fake-website detection tools' performance-related elements must be enhanced and marketed to promote their use. Particularly, tools' benefits in terms of their accuracy and speed boost users' coping appraisal and constitute critical factors in the design of detection tools. On the other hand, the perceived cost of tools' error increases users' threat appraisals. The resultant users' perceived response and self-efficacy are the pivotal coping mechanism in dealing with security threats posed by fake websites and are major conduits for transforming users' perceptions of performance-related elements into their increased reliance on such tools.

2. Theory Development

We base our theory development on the core constructs of protection motivation theory (PMT), which we contextualize to fake-website threats and tools to counter them. We extend the core PMT constructs to include tools' performance (benefit) and cost of error, users' reliance on the detector and their success in self-protection against online threats. We refer to this contextualized PMT as the detection tool impact (DTI) theory.

Whetten, Felin, and King (2009) categorize theory borrowing into two types: vertical and horizontal. Vertical borrowing changes the level of analysis and abstraction, whereas horizontal borrowing moves across contexts. We use the latter in this study. Contextualization has emerged as a valuable approach in theory development, which makes it possible to identify distinguishing features and boundary conditions of the theory (Whetten, 2009, Hong, Chan, Thong, Chasalow, & Dhillon, 2014), which enhances the borrowed theory, contributes to the emergence of context-specific theories (Whetten, 2009), and leads to a deeper understanding of the "why" and "where" of theory building (Johns, 2006).

Whetten (2009, p. 29) distinguishes between "context specificity" and "context sensitivity" of theories. Context specificity refers to the context in which the theory explains relationships among variables, making the explanatory power of theory "conditional" on a specific context. Context specificity enhances the application of a theory to new fields of inquiry. Context-sensitivity shows the sensitivity of relationships to changes in context (Whetten, 2009). There are theories and core constructs that are "paradigmatic" (as opposed to "propositional"), which are accepted lenses among the research community because of their recurrent significance in extant applications. The threat and coping appraisal constructs of PMT (Rogers, 1975; Rogers, 1983) constitute paradigmatic constructs since their saliency has been established in multiple applications in various fields including health and IS security. These constructs have demonstrated significant explanatory power in predicting security behaviors (Anderson & Agarwal, 2010; Chen & Zahedi, 2009; Johnston & Warkentin 2010).

According to PMT and theories that were built on it—most notably the technology threat avoidance theory proposed by Liang and Xue (2009)—security tools are avoidance mechanisms that help users counter threats. As positive technology stimuli, security tools directly involve users' cognitive

processes of avoiding threats and taking protective actions (Chen & Zahedi, 2009; Liang & Xue, 2009). PMT has been used in voluntary settings to study users' decisions on protective behaviors (e.g., Anderson & Agarwal 2010; Chen & Zahedi 2009). Hence, PMT constitutes an appropriate core theory to investigate users' online security behaviors.

PMT posits that humans' protective behaviors involve two cognitive processes—threat appraisal and coping appraisal. The principal variables in the threat appraisal process are the perceived susceptibility to the threat (a perception about the extent of vulnerability to the threat) and the perceived severity of the threat (a perception about the magnitude of possible harm if no countermeasures are taken). The primary constructs in the coping appraisal process are response efficacy (a belief in the effectiveness of the countermeasure) and coping self-efficacy (a belief in one's own ability to deal with the threat with countermeasures) (Rogers, 1975; Rogers, 1983).

We extend PMT by contextualizing it to fake-website threats and using detection tools to counter them. This "specific" context adds several core constructs (X in X→Y) as antecedents of PMT's threat and coping appraisals. This specificity involves benefit and cost of detection tools, which provide an opportunity to alter perceptions of threat and coping as well as consequent outcomes by manipulating detection tools' features. Another addition to context specificity in our theory is the extension of the behavior outcomes to include reliance on detection tools in decisions to visit and interact with websites and users' self-protection performance, which make the right side (Y in X→Y) context-specific. Context-specific X and Y are called Level 1 contextualization (Hong et al., 2014).

The Level 2 extension of a theory involves investigating how "sensitive" the specific theory is with respect to "where" it is implemented (Whetten, 2009, Hong et al., 2014). In fake-website threats, context-sensitivity could be explored from multiple perspectives, the more immediate of which are threat and domain types. Fake-website detection tools could embody algorithms specially designed for particular threat types and domains (type of websites with different products and services). From users' points of view, threat type and domain type could influence their perceptions and behaviors. Therefore, our Level 2 extension of PMT is to investigate the "context sensitivity" of our theory with respect to threat and domain types.

2.1. Contextualization of Outcomes

PMT proposes that, when individuals appraise the threat by assessing the susceptibility to and severity of the threat and are confident in their coping ability (in terms of response efficacy and self-efficacy), they tend to take protective actions in terms of single or multiple actions (Rippetoe & Roger, 1987) or may adopt maladaptive behaviors, such as avoidance or wishful thinking (Milne, Sheeran, & Orbell, 2000). In the IS studies that apply and extend PMT, the outcome of threat and coping appraisals has been conceptualized as behavioral intent (Johnson & Warkentin, 2010) and avoidance and emotion-focused coping (Liang & Xue, 2009).

In contextualizing PMT specific to fake-website threats and detector tools to counter them, we argue that there are two types of outcomes: reliance on a tool in dealing with fake-website threats and the success of individuals in self-protection. Individuals access the Web regularly, and in each access they need to decide whether or not the website is fake. They may rely to a varying degree on the detector in making this decision. Furthermore, the ultimate criterion for judging a detector's performance and users' behaviors is the extent of users' success in self-protection in the repeated use of the detector. Therefore, user reliance and performance constitute the contextualization of the outcome variables in the DTI theory.

2.2. Contextualization of Detector Benefit and Cost

To identify the salient elements for benefit and cost analysis of fake-website detection tools and understand user reactions to such tools, we need to look into users' cognitive process of detecting deceptions when such tools are in place. According to the competence model of fraud detection (Johnson, Grazioli, Jamal, & Berryman, 2001), a deception involves two parties with conflicting interests, a deceiver and a target. The deceiver uses deceptive tactics to manipulate and misrepresent cues of a situation that depart from the truth to induce a misjudgment by the target. The

target, therefore, will behave in accordance with the deceiver's manipulations and misrepresentations (Johnson et al., 2001). To successfully detect deceptions, individuals need to detect the inconsistencies between the cues manipulated and the truth. Thus, fake-website detection tools need to enhance avoidance behavior by improving users' propensity to notice and attribute deception (Xiao & Benbasat, 2011). More specifically, effective fake-website detection tools need to facilitate individuals' cognitive process in arousing suspicion(s) about abnormalities (inconsistencies between the cues manipulated and the truth), generating and evaluating hypotheses on the situation, and reaching a conclusion about whether there is a deception (Johnson et al., 2001). In fake-website detection, two broad categories of tool elements can facilitate such cognitive process: (1) performance (benefit) and cost elements and (2) user interface elements. Performance and cost elements play a critical role in activating users' fraud detection cognitive process before they fall into the deceiver's manipulations; user interface elements communicate the tool's findings and help users detect manipulated and misrepresented cues and heed the tool's warnings.

This paper is part of a larger federally funded research project that investigates both the performance (benefit)/cost and user-interface elements of fake-website detection tools. In this paper, we report on the first category of elements. Table 1 summarizes a selective set of studies relevant to our study. As we elaborate below, based on the literature, we have identified salient performance-related elements for fake-website detection tools as detector' accuracy and runtime speed, which constitute the benefits that users will derive from using such tools. However, no tool is perfect. Tools' errors could cost users in terms of financial damage or efforts to mitigate consequences of such errors; hence, perceived cost of error is a salient element.

Table 1. Contextualization of Fake-Website Threats and Detection Tools

Study	Method	Study objective	Performance metrics	Findings
Benefit: *performance: accuracy and runtime speed*				
Abbasi et al. (2010)	Experiment	Improving detection accuracy for fake website detection	Overall accuracy, class-level precision, & class-level recall	AZProtect using SLT-based algorithm is more accurate in detecting both spoofed and concocted fake websites
Bliss, Gilson, & Deaton (1995)	Experiment	Investigating the match between (i) warning reliability and (ii) users' response frequency, speed, and accuracy	Warning reliability, response frequency, speed & accuracy	90% of the subjects' response frequency to the warnings matched the warning reliability
Jonsson, Harris, & Nass (2008)	Experiment	Studying impacts of accuracy of an in-car hazard warning system on driving performance	# of collisions & offroad accidents, obeying traffic laws, & perceived accuracy	Decreased accuracy of the system negatively impacted driving performance and trust in the system
Zhang et al. (2007)	Experiment	Comparing the accuracy of 10 popular fake website detection tools	Class-level recall	No single detection technique emerged, tools' performance varied depending on the data sources
Cost: *cost of detector's error*				
Cavusoglu, Mishra, & Raghunathan (2005)	Mathematical modeling	Studying the organizational value of using detection systems based on a cost-benefit model	Damage caused by an undetected intrusion, cost of manual investigation, and utility of intrusion detection	Using intrusion detection systems had positive values for organizations

Table 1. Contextualization of Fake-Website Threats and Detection Tools (cont.)

Study	Method	Study objective	Performance metrics	Findings
Cost: *cost of detector's error*				
Yue and Çakanyildirim (2007)	Mathematical modeling	Comparing the response cost of clearing intrusion alarms when using reactive vs. proactive response strategies	Response costs and damage costs	An optimal response strategy is a mixture of both reactive and proactive responses and depends on cost and investigation rate parameters
Threat context-sensitivity				
Abbasi et al. (2010)	Experiment	Improving fake-website detection accuracy using learning classifiers that use more fraud cues and threat type information	Performance measures including overall accuracy, class-level precision, and class-level recall	AZProtect using SLT-based algorithm is more accurate in detecting both spoofed and concocted fake websites when threat type cues were fed into the algorithm
Abbasi & Chen (2009b)	Experiment	Studying impacts of threat type-specific cues on fake website detection performance	Overall accuracy and class level F-measure, precision, and recall	Rich threat type-specific cues along with a proper choice of algorithms can improve detection performance of fake escrow websites
Lau et al. (2011)	Experiment	Improving online review deception detection accuracy by incorporating threat-type-specific deception cues	Class-level misclassification rates	Using threat type- specific cues can improve detection performance of online review deception
Domain context-sensitivity				
Biros, George, & Zmud (2002)	Experiment	Studying how domain experience and other focal factors impact deception detection rate, false alarms, and task accuracy	Deception detection rate, false alarms, and task accuracy	Domain experience was positively associated with task accuracy
Grazioli & Jarvenpaa (2003)	Content analysis	Investigating the deceptive tactics used by deceivers on the Internet in different domains	Distributions of deception tactics used in three domains: b2b, b2c, and c2c	Different types of deceivers used different deceptive tactics in different domains.
Johnson et al. (2001)	Field experiment	Studying impacts of involving cognitive processes to successfully evaluate domain-specific deceptive tactics	Domain-specific deceptive tactics and cues, & detection errors	Employing the proposed heuristics model (based on the competence model of fraud detection) successfully detected frauds in the cases.

2.2.1. Benefit: Detector's Accuracy and Speed

In many cases, security tasks are "secondary" to many users. They want the security task to get done as quickly as possible so that they can go back to the primary task (Dhamija, Tygar, & Hearst, 2006). Therefore, security decisions are made under time pressure because they distract users from their primary task. To help users make fast and accurate security decisions about visiting a website,

detection tools should be able to provide timely and accurate detection results. With respect to accuracy, the two types of errors associated with alarm systems are failing to detect a fake website (alarm failures) and false alarms (Bliss et al., 1995; Edworthy, 1997). It has been reported that existing fake-website detection tools suffer from significantly high alarm failures (i.e., low detection rates of fake websites) (Zhang et al., 2007; Abbasi & Chen, 2009a). This is quite problematic since the potential consequences of alarm failures can be quite devastating in terms of financial loss and identity theft (Abbasi et al., 2010). Researchers have endeavored to develop algorithms for detection tools that can deliver accurate and timely detection results (Abbasi et al., 2010). Therefore, accuracy and speed of detector tools should be among the salient elements impacting users' security behaviors.

2.2.2. Cost: Perceived Cost of Detector's Error

Detection tools are evaluated based on their benefit and cost. Tools' benefits stem from their ability to detect fake websites, but their costs include the extent of users' loss caused by the tools' inability to accurately detect the threat and the monetary consequences of such errors (Cavusoglu et al., 2005; Abbasi et al., 2010). By following a detector's false negative advice (failing to warn against a fake-website attack), users could suffer costly damages such as identity theft (Dinev, 2006). Such failures impact users' cost-benefit evaluation about a threat countermeasure (e.g., a detection tool) (Liang & Xue, 2009). Considering that designers of detection tools can incorporate false negative costs (in the detection methods) that are congruent with users' perceptions, a deeper understanding of the impact of error costs on user perceptions and behaviors is warranted; hence, cost of detector error is a salient element.

2.3. Threat Context-Sensitivity: Type of Threat the Detector Can Handle

Two prevalent types of fake websites that employ contrasting forms of deception (i.e., attack strategies) are spoofed and concocted sites. These varying types of deception have important implications for detecting fake websites (Xiao & Benbasat, 2011). Spoofed sites mimic well-known existing websites. The purpose of these sites is online identity theft (Abbasi et al., 2010). Concocted sites are deceptive websites attempting to appear as unique, legitimate online entities with the objective of failure-to-ship fraud (Chua & Wareham, 2004; Abbasi et al., 2010). Currently, concocted sites are becoming increasingly common, with thousands of new examples appearing daily on the Internet (Airoldi & Malin, 2004; Greenberg, 2008). The two types of fake websites use different deceptive tactics for successfully defrauding Internet users (Grazioli & Jarvenpaa, 2003). Consequently, users may behave differently when using detection tools in the context of spoofed websites as compared to concocted websites. For instance, users often discount tool recommendations when encountering spoofed websites that "appear familiar" (Wu et al., 2006). Moreover, these two types have important implications for the design of fake-website detection tools. Prior studies have noted that, due to the differences in the fraud tactics, many existing tools focus on detecting only a single category and so provide limited support across both spoofed and concocted sites (Abbasi et al., 2010). This limitation, coupled with the potential for variation in user behavior when encountering spoofed and concocted websites, underscores the significance of including the threat type as a salient element impacting users' behaviors.

2.4. Domain Context-Sensitivity: Type of Domain the Detector Can Handle

Prior studies have demonstrated the influences of domain of use on Internet users' behaviors. Internet users' decision to disclose private information depends on the website domains (Bansal, Zahedi, & Gefen, 2008). In highly sensitive domains such as health and finance, users could show "visceral feelings" about their private information and be reluctant to disclose (Angst & Agarwal, 2009, p. 359). However, this might not be the case in relatively insensitive domains such as online news. Meanwhile, even in highly sensitive domains such as online pharmacies or online banks, users might have different threat and deception awareness based on their personal experiences and domain knowledge (Kumaraguru et al., 2010). For instance, fake online pharmacies are highly successful due to Internet users' general lack of awareness about medical content pertaining to FDA regulations, warnings regarding adverse drug reactions, and the prevalence of rogue Internet pharmacies (Greenberg, 2008; White & Horvitz, 2009; Abbasi et al. 2012). Therefore, it is essential to study the role of detection tools for the domains in which users have greater security concerns.

3. Model Conceptualization and Hypothesis Development

Based on the DTI theory, we propose our conceptualized detection tool impact (DTI) model (See Figure 1). Table 2 summarizes the constructs' definitions. The model is a user-centric assessment of how salient elements of the detection tool could change users' reliance on the tool and their self-protection performance.

According to PMT, individuals first appraise a threat (threat appraisal) and then assess ways to cope with it (coping appraisal) (Liang & Xue, 2009). Coping appraisal includes individuals' assessment of their own abilities (self-efficacy) and the efficacy of response to the threat (response efficacy). During the coping appraisal, individuals form their perceptions about the effectiveness of the countermeasures and then consider personal effectiveness.

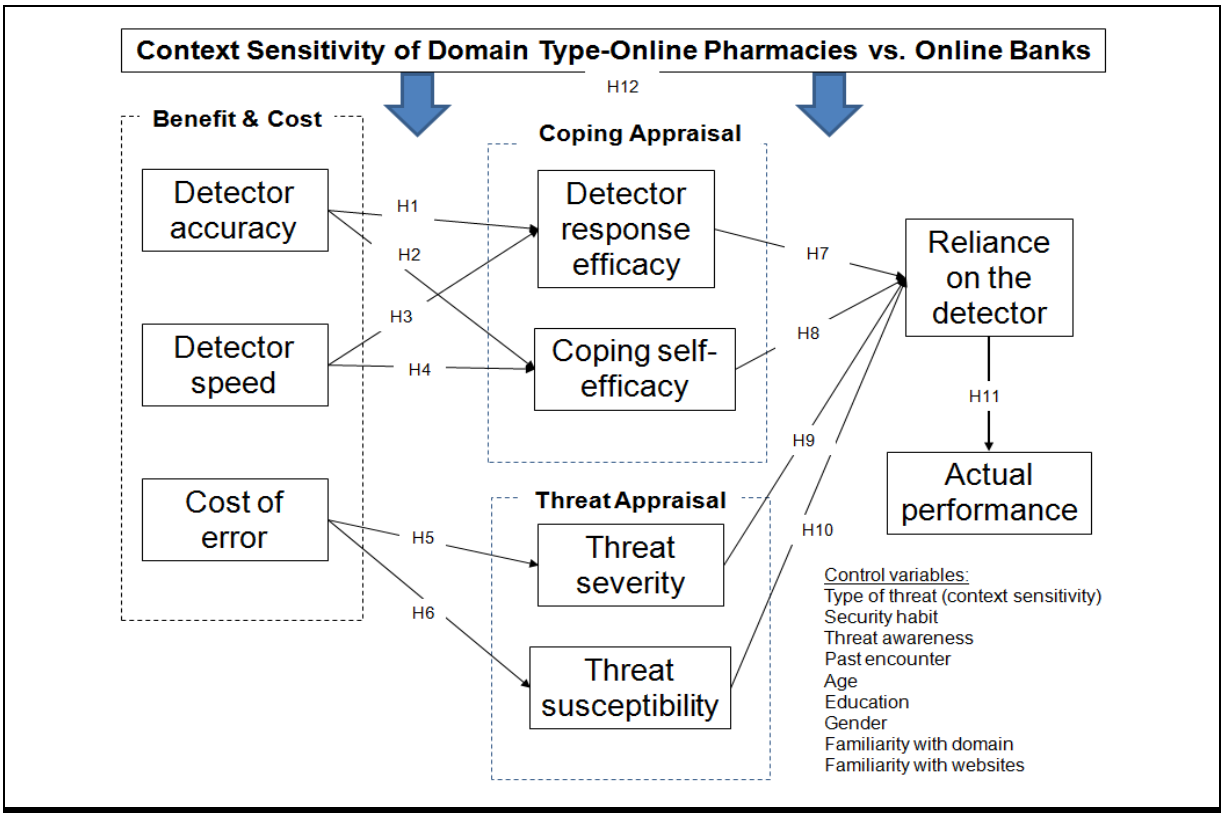

Figure 1. Detection Tool Impact (DTI) Model

Table 2. Construct Definition and Source of Scale Development

Constructs	Definitions	Major references
Detector response efficacy	Users' belief about the effectiveness of the tool in detecting fake websites	Liang & Xue (2009), Johnston & Warkentin (2010), Rogers (1975), Witte, Cameron, McKeon, & Berkowitz (1996)
Cost of detector error	Users' perceptions regarding the financial loss caused by the detector errors	Rovira, McGarry, & Parasuraman (2002), Virta, Jacobson, & Kobza (2003)
Coping self-efficacy	Users' beliefs of their own ability of taking security countermeasures to deal with fake website threats	Bandura (1982), Rogers (1975), Witte et al. (1996)
Perceived threat severity	Users' beliefs about the magnitude of the potential harm caused by visiting fake websites	Johnston & Warkentin (2010), Liang and Xue 2009; Rogers 1975; Witte et al. 1996
Perceived threat susceptibility	Users' beliefs about their personal possibility of encountering and/or visiting fake websites	Johnston & Warkentin (2010), Liang & Xue (2009), Rogers (1975), Witte et al. (1996)
Reported reliance on the detector	Users' decision to follow the recommendation of the detector in making decisions regarding visiting or transacting with a website	Davis (1989), Straub, Limayem, & Karahanna (1995), Venkatesh, Morris, Davis, & Davis (2003)
Actual performance	Users' actual success in identifying and avoiding fake website attacks	Wu et al. (2006), Dhamija et al. (2006), Adipat, Zhang, & Zhou (2011)

Applications of PMT have shown that threat appraisal and coping appraisal are two cognitive mediating processes in individuals' protective behaviors in health contexts (Rippetoe & Rogers, 1987). In contextualizing PMT, the DTI theory argues that, in coping appraisal for dealing with fake website threats, users need to rely on the efficacy of both detection tools and their own coping abilities in dealing with the threat.

Per the DTI theory, the detector's performance elements are accuracy and speed, which benefit its users. A tool's response efficacy is an important component of coping appraisal because an effective tool that can identify and prevent fake-website attacks gives users peace of mind when visiting the Web. A protective IT artifact's ability to accurately detect threats impacts users' perceptions of the artifact (Sunshine et al., 2009). In the context of fake websites, less accurate detectors have been associated with lower perceived response efficacy (Li & Helenius, 2007; Abbasi et al., 2010). "Warning fatigue", "crying wolf", and "alarm failure" are all examples of observed low perceived response efficacy effects attributable to poor detector accuracy (Bliss et al., 1995; Egelman, Cranor, & Hong, 2008; Sunshine et al., 2009; Akhawe & Felt, 2013). Conversely, other studies have shown that higher detector accuracy can improve perceived detector response efficacy (Wu et al., 2006; Herzberg & Jbara, 2008). Thus,

H1: *Detector's accuracy is positively associated with users' perceived detector response efficacy.*

Self-efficacy is defined as beliefs about "one's capability to organize and execute the course of action required to produce attainment" (Bandura, 1997, p. 3). Self-efficacy has been shown to promote various behaviors (Bandura, 1982; Bandura, Adams, & Beyer, 1977) and appears in PMT as a part of coping appraisal. Due to the limitation of resources available for an action (such as paying attention to the advice of a detector while engaged in a primary task), a cost-benefit evaluation of taking the action could also improve or diminish self-efficacy (Bandura, 1982; Bandura et al., 1977; Marks & Allegrante, 2005; Strecher, DeVellis, Becker, & Rosenstock, 1986). Performance achievement is one

of the major sources of self-efficacy. Success gives people a sense of mastering the situation (Bandura et al., 1977). The literature in health-related behaviors shows that individuals' self-efficacy could be enhanced through deliberate manipulations, which subsequently lead to behavior improvements in areas such as smoking cessation, weight control and alcohol abuse (see Strecher et al. (1986) for a review). Furthermore, Compeau and Higgins (1995) have shown that individuals' computer self-efficacy can be improved by others' encouragement, use, and support. Similarly, Lam and Lee (2006) have shown that others' encouragement and support influence internet self-efficacy for older adults. Extending these arguments to detection tools, we argue that the accuracy of the tool influences users' coping self-efficacy since a more accurate tool provides users a stronger sense of ability to cope with online threats. Thus,

H2: *Detector's accuracy is positively associated with users' coping self-efficacy.*

Prior studies have recognized the importance of detector run-time on user perceptions of the tool (Xiang, Hong, Rose, & Cranor, 2011). Simply put, faster tools have been considered superior performers (Chou, Ledesma, Teraguchi, Boneh, & Mitchell, 2004). Run-time speed has been one of the major metrics for measuring the performance of detection tools mostly due to the secondary nature of fake-website detection in real-time user environments (Abbasi et al., 2010). When the detector has a long process time, it could interfere with individuals' primary purpose for visiting websites, costing them time and focus while waiting for the detector to run and return its results (Dhamija et al., 2006). As Kumaraguru et al. (2010) note, "one does not go to an online banking Web site to check the SSL implementation of the Web site, but rather to perform a banking transaction" (p. 2). Consequently, in real-time detection environments with users constantly awaiting tool recommendations, fast run-time speed is "crucial" for maintaining favorable user perceptions of tool performance (Abbasi & Chen, 2009b, p. 100). Hence,

H3: *Detector's run-time speed is positively associated with users' perceived response efficacy*.

Humans strive to have control over their environments. Self-efficacy enables them to exercise personal control (Bandura, 1997). Control over time has been shown to play a major role in workers' stress, satisfaction, and performance in organizational studies (Macan, 1994), which has led to the concept of "time congruity" (Francis-Smythe & Robertson, 2003). Time congruity is the agreement between individuals' style of using time with the time demand under which they work. Studies have shown that interruptions (such as those caused by supervisors) lead to the perception of poor time control (Francis-Smythe & Robertson, 2003; Chen, Zhang, Leung, & Zhou, 2010). Applying these findings to the context of fake-website detectors, we argue that the run time of the detector is an interruption that can reduce individuals' time congruity in performing their primary tasks of web access and use. A detector's fast runtime reduces the extent of this interruption and, hence, preserves individuals' time congruity and promotes a sense of control over their environment, which, in turn, positively influences their coping self-efficacy. Thus,

H4: *Detector's speed is positively associated with users' perceived coping self-efficacy.*

The PMT assumes that people indeed assess expected benefits and costs and that this assessment plays a role in their threat appraisal (Rippetoe & Rogers, 1987; Weinstein, 1988). Cost includes the "effort in carrying out a precaution, the expense, any undesirable side effects" (Weinstein, 1988, p. 365). In the DTI theory, one side effect of using the detector is the perceived cost of its error. Hence, we argue that the assessment of cost due to detector error is a part of the cost-benefit analysis, which initiates threat and coping appraisals because people tend to first make more general cost assessments of a protective action and then move to more personally related assessments such as whether they are exposed to a given threat in terms of the severity of and susceptibility to the threat (Weinstein, 1988).

The cost of detection error is damaging to those who follow the system's incorrect recommendations (Cavusoglu et al., 2005). Models for detecting security threats have often leveraged perceived misclassification costs, which are closely aligned with perceived threat severity (Lee, Fan, Miller,

Stolfo, & Zadok, 2002). For instance, in the context of intrusion detection systems (Lee et al., 2002; p. 6), the perceived cost of detection error is related to the perceived "cost of damage caused by an intrusion." Similarly, perceptions about costs of a failure to detect a phishing email are related to the perceived severity of the attack (Abu-Nimeh, Nappa, Wang, & Nair, 2007). Consequently, users' perceived costs associated with detection errors impact their perceptions about the severity of the threat. Hence,

H5: *Perceived cost of detector error is positively associated with users' perceived threat severity.*

Research has found that automatic tools' errors can impact users' perceptions of the tools' creditability and capability and the users' consequent behaviors (Rice, 2009). According to PMT, an assessment of expected costs when taking the recommended countermeasure plays an influential role in users' cognitive processes of making decisions about the threat (Rippetoe & Rogers, 1987; Weinstein, 1988). In the specific context of fake-website detention tools, the DTI theory posits that cost of detector error triggers users to reassess their vulnerability to fake website threats. Higher perceived costs reduce users' beliefs that the protective tool will safeguard them (Liang & Xue, 2009, 2010). The uncertainty caused by perceived cost of error adds to the perceived likelihood of threat and increases users' anxiety about their threat exposure because they have to contend with two sources of threat: fake-website threat and threat of costly error. Thus, perceived cost of error can compound users' sense of being vulnerable and defenseless against attack.

H6: *Perceived cost of detector error is positively associated with users' perceived threat susceptibility.*

One of the two dependent variables in this study is the extent of reliance on the tool as reported by users. While intention to use IT artifacts has been a commonly used dependent variable in studying users' behaviors and IT adoption, for security tools, actual use is the gold standard. Taking precaution against a threat is a decision and has a dynamic process (Weinstein, 1988). Expressing intention does not necessarily capture the decision in the hazard condition when an individual actually comes face to face with a specific threat because "many people who claim to be convinced that a precaution is worthwhile, admit that they have yet to carry through on their intentions" (Weinstein, 1988, p. 374). Weinstein (1988) gives an example of individuals who intend to stop smoking but never carry out the intention until coming face to face with the specific threat of lung cancer. Contextualizing this argument for using the detector as a precaution, we argue that the actual reliance on a detection tool in a specific condition of threat is a more salient measure of actual use. Hence, reported reliance in this study refers to the individual's decision to follow the recommendation of the tool in making decisions regarding visiting or transacting with a website.

In PMT, the threat appraisal (threat susceptibility and severity) as well as coping mechanism (coping self-efficacy and response efficacy) are behavior antecedents. In the DTI theory, these core constructs impact the context-specific outcomes—users' reliance on the detector, which, in turn, influences users' self-protection performance. Hence, we posit that threat appraisal and coping appraisal influence users' reliance on the detector. Detector response efficacy represents users' beliefs that the tool is effective and accurate. As a coping mechanism, an effective tool should encourage more use. In design science it has been observed that "users should have accurate beliefs about the reliability of automation" (Parasuraman & Miller, 2004, p. 52). In the IS field, numerous studies have demonstrated that a reliable tool is an important antecedent for use and intention to use the IT artifact (e.g., McKnight, Choudhury, & Kacmar, 2002; Vance, Elie-Dit-Cosaque, & Straub, 2008; Zahedi & Song, 2008). In the context of online security, one can argue response efficacy is a salient measure of the reliability of a detection tool. Specifically in the context of fake websites, perceived detector response efficacy has been theorized as a likely predictor of tool reliance (Cranor 2008). Users with low perceived detector response efficacy may choose to ignore or disregard tool warnings (Egelman et al., 2008). A recent large-scale fake-website detection study suggests that users' reliance on detection tool warnings can vary by between 40% and 60% purely based on their perceived detector response efficacy (Akhawe & Felt, 2013). Hence,

H7: *The extent of users' reported reliance on the detector is positively associated with perceived detector response efficacy.*

Self-efficacy is "the strength of convictions" in one's own ability, which determines whether "coping behavior will be attempted" (Bandura, 1982; Bandura et al., 1977, p. 126). Numerous studies have shown that self-efficacy in taking protective actions to deal with a threat is an antecedent of behavioral change (e.g., Rippetoe & Rogers 1987; Witte et al., 1996) and a major determinant of security-related behaviors (Anderson & Agarwal, 2010; Chen & Zahedi, 2009; Johnston & Warkentin, 2010; Liang & Xue, 2009). Specifically in the context on security warnings, self-efficacy has also been theorized as having a positive relation with security tool reliance (Cranor, 2008). Thus,

H8: *The extent of users' reported reliance on the detector is positively associated with their perceived self-efficacy.*

It is observed that people will not take protective actions against a threat unless they feel vulnerable (Weinstein, 1988; Witte et al., 1996). Therefore, we should expect that higher levels of threat susceptibility and severity should prompt individuals to rely more on the detector's recommendation (Anderson & Agarwal, 2010; Chen & Zahedi, 2009; Johnston & Warkentin, 2010; Liang & Xue, 2009). The influence of threat severity on reliance stems from the argument that, as the magnitude of harm caused by visiting fake websites increases, users are more likely to seek to protect themselves by relying on the detector. There is evidence in the fake-website detection literature to support this argument. Downs, Holbrook, and Cranor (2007) observed that, when encountering fake websites, users with higher perceived threat severity for having their information stolen were more likely to take protective actions. Egelman et al. (2008) performed a qualitative analysis of users that relied heavily on fake-website detectors and found one of the most common user-reported reasons to be high perceived threat severity, with responses such as: (1) "didn't want to get burned", (2) "don't like to gamble with the little money I have", and (3) "better to be safe than sorry". In general, when encountering a potential fake-website, users' perceptions of the threat, and the resulting judgments, are critical pre-requisite considerations to any protective behavior such as detector reliance (Camp, 2009; Bravo-Lillo, Cranor, Downs, & Komanduri, 2011). Hence,

H9: *The extent of users' reported reliance on the detector is positively associated with perceived threat severity.*

Threat susceptibility is another component of threat appraisal. People normally do not pay attention to adverse events that they perceive as rare or unlikely to impact them (Rogers, 1975). Similarly, "if an IT threat is perceived to have no chance of occurring, there should be no interest in acting against it" (Liang & Xue, 2009, p. 81). Perceived vulnerability to fake-website attacks is considered an important variable impacting users' likelihood of taking protective actions (Downs, Holbrook, & Cranor, 2006). When using security tools to protect against fake-websites, low perceived threat susceptibility has been observed as a major cause for ignoring or disregarding tool warnings (Wu et al., 2006). Users have to feel vulnerable to a fake-website threat in order to pay attention to the detector's warnings and follow its advice. Thus,

H10: *The extent of users' reported reliance on the detector is positively associated with perceived threat susceptibility.*

In the literature of security research, the users' performance when using a protection tool is rarely assessed. Some studies have developed models to assess system performance when using protective resources (Basagiannis, Katsaros, Pombortsis, & Alexiou, 2009). It also has been reported that not using tools that prevent security attacks resulted in spoof rates as high as 30-45 percent (Wu et al., 2006). However, to our knowledge, there has not been any study on developing conceptual models for assessing individual security performance when using detection tools. We address this gap by including users' performance assessment as the second dependent variable in our model. We argue that security performance enhancement is the ultimate goal of developing any security tool. People generally are poor at detecting deceptions; relying on tools could help improve their detection rates (Biros et al., 2002; DePaulo, Stone, & Lassiter, 1985). Thus, using the detection tool in making

decisions about visiting a website or transacting with the website should improve users' performance in avoiding the fake-website security threats. Hence,

H11: *Users' actual performance in avoiding fake websites is positively associated with the extent of reported reliance on the detector.*

3.1. Context-Sensitivity of Domain and Threat Types

Whetten (2009) distinguishes between "specificity" and "sensitivity" of context in theory building (p. 29). In our case, while the DTI theory is "specific" to online security threats and the role of detection tools in preventing them, its "sensitivity" should be tested within different types of domains in which people feel threatened and may rely on the detector to prevent security threats. People use the Web for different purposes and tasks, some of which are more sensitive and critical than others. Consequently, Internet users' security-related perceptions and behaviors may vary depending on web domains (Angst & Agarwal, 2009; Bansal et al., 2008). In our case, due to differences in the nature and impacts of website frauds in online banks and pharmacies (Armin, 2010, Easton, 2007; Lennon, 2011), users may be more sensitive to online banks than online pharmacies since they may suffer immediate financial loss from fake online banks.

Following Johns (2006), we define domain type as "situational opportunities and constraints" that could influence individuals' security behaviors and "functional relationships between variables" (p. 386). Domain type establishes the "when" aspect of theory building—one of the omnibus dimensions of context identified by Johns (2006), and constitutes the condition under which strengths of relationships in DTI theory are examined. Per Whetten (2009), the DTI theory is a "conditional" explanation in that use domain could modify the benefit and cost impact of the detector and users' eventual reliance on it. Whetten (2009) argues that, if a variable (Z) measuring context-sensitivity impacts X (in X→Y), then it should be conceptualized as a moderator, whereas if Z impacts only Y, then it should be used as a control variable.

We use two variables to study the context-sensitivity of our theory: domain type and threat type. People use the Internet in different domains for different purposes. A sensitive domain involves the exchange of people's sensitive private information. Security attacks in such domains could pose serious monetary or personal damages. We posit that people's perceptions and behaviors are affected by the sensitivity of the domain. Therefore, domain should moderate the paths in the model. In accessing a sensitive website, users tend to have a high degree of awareness about the type of website domain. Research has shown that when users access websites in sensitive domains, they feel more vulnerable (SAP, 2013). We argue that users' acute awareness of domain type influences their expectation of detection tools' benefits and costs. For example, users who have online bank accounts are far more aware of the fake-website threats to their finance, and, hence, expect a higher level of performance from detection tools in order to use them. Hence, we investigate context-sensitivity of domain type as a moderator of the DTI paths.

We explore this moderation through concentrating on two important domains: online pharmacies and online banks. We selected these domains since health- and money-related activities are both sensitive domains with significant online activity and prevalence of fake website-based fraud. Internet fraud often occurs as a result of unsuspecting Internet users providing personal information to fake websites in exchange for fictitious products and/or services (Chua & Wareham, 2004; Abbasi et al., 2010, 2012). Financial institution websites are among the most common domains for fake website attacks (Ramzan & Wuest, 2007). For instance, fake online banks are highly successful at luring victims using the ruse of offering attractive escrow services, bank accounts, currency exchange, small business loans, philanthropic ventures, and so on (Abbasi & Chen, 2009b). Similarly, fraudulent online pharmacies are highly pervasive. According to studies conducted by the World Health Organization and U.S. Food and Drug Administration, 11,000 of the 12,000 online pharmacies examined were websites engaging in a variety of fraudulent activities, including failure-to-ship, identity theft, and sale of counterfeit products; and the number of people visiting such websites continues to increase dramatically (Krebs, 2005; Easton, 2007; Greenberg, 2008).

In the case of online banks, the financial loss due to fake-website attacks is more immediate and impactful. Cash thefts from individual accounts could be discovered faster and are more visible, whereas, in the case of online pharmacies, there are a variety of impacts such as non-delivery, identity theft, and exposure to fake drugs, which are less visible and could take longer to discover.

Therefore, depending on the immediacy and consequences of attacks, individuals may have different appraisals of threats and their coping capabilities. The way individuals behave in one type of domain may not necessarily be the same as their behavior in a different domain type. Therefore, domain type could moderate the impacts the detector's cost and benefit on individuals' appraisals of threats and coping efficacy as well as the paths leading to their reliance on the detector. The moderating influence of domain type on the model paths is exploratory at this point since the conditional manifestations of such moderation are yet to be explored.

H12: *Domain type, online banks vs. online pharmacies, moderates the DTI paths.*

When it comes to threat type, users have little knowledge of threat types and the ways fake websites could deceive them. Therefore, users' expectations of benefit and cost of detection tools or their perceived threat and coping appraisals could not be influenced by threat type. However, detection tools' success in dealing with the two threat types may differ. The variance in detection performance influences users' self-protection success; thus, threat type impacts Y only. Following Whetten's (2009) argument, we use threat type as a control variable that impacts users actual performance.

3.2. User Profiles as Control Variables

In a user-centered design approach, identifying and understanding user profile variables and individual differences that play a role in users' perceptions and behaviors regarding system design features are critical to the successful design of personalized systems (Kramer, Noronha, & Vergo, 2000). In the IS behavior literature as well as the PMT literature, demographic variables, including age, gender, and education are included as profile variables (e.g., Venkatesh et al., 2003). Age has been shown to be a salient factor in the application of PMT (Sturges & Rogers, 1996). Experience-related individual differences, including past encounters with fake websites and familiarity with the domain and websites, are also part of user profiles (Bansal, Zahedi, & Gefen, 2010; Chen & Zahedi, 2009; Zahedi & Song, 2008). Security habit, defined as users' routine security behaviors without conscious intention, is an influencing factor impacting users' security perceptions and behaviors (Pavlou & Fygenson, 2006). In Weinstein's (1988) study, survey respondents reported "not habitual" as the one of the main reasons for not carrying out precaution intentions. Habit contributes to the sense of coping self-efficacy. We therefore included security habit as a control variable in users' profiles. Moreover, the literature on threat perception indicates that threat awareness plays a significant role in security behavior (Dinev & Hu, 2007; Straub & Welke, 1998) and is associated with the perception of susceptibility to a threat (Smerecnik, Mesters, de Vries, & de Vries, 2009). We have included the awareness as a control associated with susceptibility.

4. Research Methodology

4.1. Experimental Design and Protocol

The research methodology was controlled lab experiment. We chose this methodology in order to examine the actual behaviors of individuals in using the detector. The experimental design was a 2 x 2 x 2 x 2 x 2 = 32 full-factorial design: tool's accuracy, tool's runtime speed, loss due to tool's error, domain type, and threat type. Each factor had two levels. The detection tool's accuracy was high vs. low (90% vs. 60%), the runtime was fast vs. slow (1 vs. 4 seconds), the loss due to the detection error was high vs. low ($10 vs. $1), the domain types were online pharmacies vs. online banks, and the type of threat was either spoofed or concocted. Each subject was randomly assigned to one of the 32 settings.

We chose the accuracy rates based on recent benchmarking studies reporting that the accuracies for commonly used state-of-the-art anti-phishing tools range from approximately 60 percent to 90 percent (Abbasi et al., 2010). This range encompasses the tools employed by the Internet Explorer and

Firefox web browsers, which collectively account for nearly 80 percent of the browser market share (Vaughan-Nichols, 2011). Since these commonly used tools have negligible false alarm rates (Abbasi & Chen, 2009a), the errors associated with the 60 percent and 90 percent accurate detectors were primarily alarm failures (i.e., failing to detect a fake website). We chose the times (1 and 4 seconds) based on existing anti-phishing tools that have run times ranging from just under 1 second to slightly over 3 seconds (Chou et al., 2004; Abbasi & Chen, 2009a). Median losses attributable to fake websites range from approximately $300 for those suffering only direct monetary losses to $3,000 for those that are also victims of identity theft, with the latter number including remediation and reputation costs (Lennon, 2011; McAfee, 2011b). To operationalize these two possible costs (i.e., low: $300 and high: $3000), we provided subjects with a virtual cash box of $100 and a damage cost (per error) of either $1 or $10. Subjects could incur total losses up to $200, resulting in a final cash box balance between -$100 and $100. Such a range of cash box values, which included the possibility of negative balances, was adopted since losses attributable to fake websites can often extend beyond the victims' current means (Lennon, 2011; McAfee, 2011b).

At the end of the experiment, subjects were made aware of their remaining cash box balance. These cash box and cost values allowed the proportions of low to high costs and between costs and median U.S. household income to be preserved while using numbers that were easier for the subjects to understand. The threat type was not part of the manipulation. Per the theoretical discussion, the threat type was included as a control variable to examine whether behaviors in response to the tool's salient elements varied based on the type of threat (spoofed vs. concocted).

We conducted the experiment in two domain types: online pharmacies and online banks. An inventory of 15 spoofed, 15 concocted, and 15 legitimate online pharmacies was identified—a total of 45 online pharmacies. The URLs for the legitimate, concocted, and spoofed pharmacy websites were obtained from reputable sources including the National Association of Boards of Pharmacy (www.nabp.net), LegitScript (www.legitscript.com), and PhishTank (www.phishtank.com). The web pages associated with each website URL were collected using a spidering program that preserved the original link structure, content, and images. An inventory of 15 spoofed, 15 concocted, and 15 legitimate online banks was also created—a total of 45 websites. The URLs for the legitimate, spoofed, and concocted online banks were obtained from reputable sources including Federal Deposit Insurance Corporation (FDIC), (www.fdic.gov), PhishTank (www.phishtank.com), Artists Against 4-1-9 (http://wiki.aa419.org) and Escrow Fraud Prevention (http://escrow-fraud.com/).

To balance subjects' familiarity with legitimate websites and avoid the company-size bias, the legitimate online pharmacies and online banks had an equal number of large, medium and small companies. Size was determined based on sales revenue for pharmacies and total dollar amount of deposits for banks. In other words, legitimate websites included approximately five from the top 10-20, another five from the middle, and five smaller companies.

Data for the two domains was collected in two rounds of data collection since the experiment included domain-specific tasks and utilized surveys that had domain-specific questions (such as familiarity with websites). Combining the two domains could create confusion in training the subjects prior to the experiment. We made sure that there was no overlap between subjects participating in the two rounds of data collection.

The entire experimental process was developed from scratch in an integrated environment using Java programming language. The experimental stimulus was developed from scratch using Java programming to simulate different conditions of fake website attacks and different tool settings in terms of accuracy, speed, cost of error, domain, and threat type. Figure 4 shows an example of the detection interface. Note that, in each case, the URL was shown to the user but is masked in this figure.

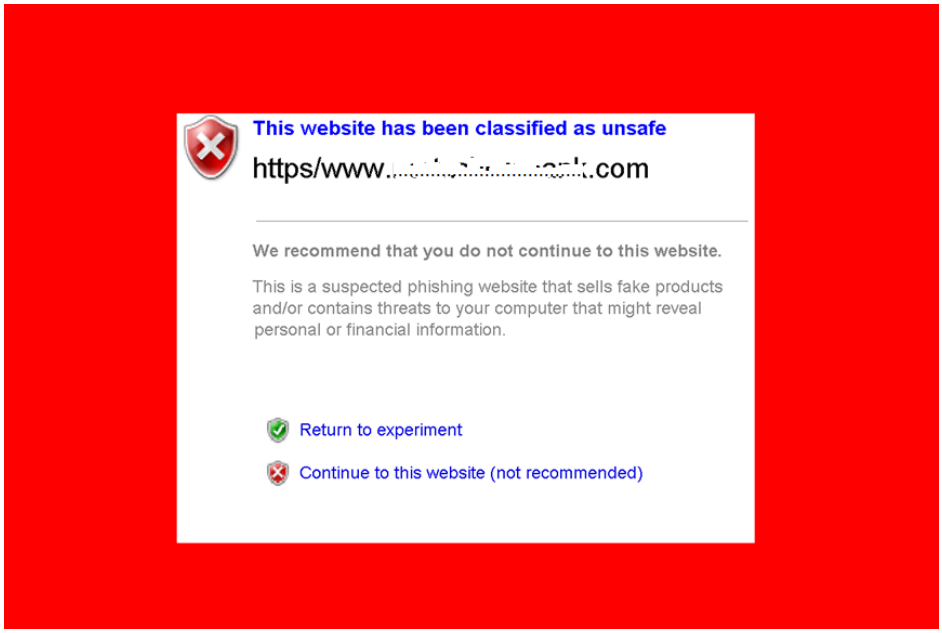

Figure 2. An Example of the Detection Interface (the URL is Masked)

For the online-pharmacies domain, the performance of fake-website detector was based on one of the 16 possible designs. The designs were randomly assigned to the participants. Prior to the start of the experiment, the participants were trained about the domains, the sequence of the experiment and the detection process.

The participants were randomly assigned to 10 websites (5 legitimate and 5 fake—either spoofed or concocted). The experimental task was to buy an over-the-counter drug with a value of about $30 (Rogaine, a hair regrowth product), for grandpa. This product was chosen because it is an over-the-counter product with which people are familiar (or could quickly be made familiar), and its counterfeits are commonly sold by fake online pharmacies at a lower price. For each website, after being exposed to the tool's recommendation, participants had to decide if they would visit the website, and once on the website, the participants had to decide if they would explore the website to find the product and, once found, if they would buy the product.

For the online-banks domain, the experimental task was to open a saving account. This is a relevant and basic function available on most online banks. Providing personal and financial information to a fake website poses great risk of financial loss and identity theft. Accordingly, for each assigned bank website, the participants had to make three decisions: whether the website was real or fake, whether the website allowed one to open a saving account (if they visited), and whether they would open a saving account with this online bank (if it allowed one to open a saving account online).

The experimental protocol was intended to mimic real conditions of use with respect to time limitation and possible loss. The participants had 20 minutes to make all their decisions regarding their 10 assigned websites. This time constraint was chosen after pre-testing and pilot testing in order to mimic the time limitation for making decisions and to ensure that the allotted time was reasonable for making threat assessment.

Visiting and transacting with phishing websites have costly consequences, such as failure-to-ship fraud, identity theft, and exposure to viruses and malware (Dinev, 2006). Incentives or disincentives are also important in motivating people to take the proper security precautions (Cranor, 2008). Therefore, participants were informed in advance that they would be awarded based on their performance. Participants' performances were scored objectively based on their 20 decisions regarding their assigned websites: (1) ability to differentiate 10 legitimate websites from fakes

(Dhamija et al., 2006; Wu et al., 2006), (2) decision to visit or avoid 5 fake websites, and (3) willingness to transact with 5 fake websites (Grazioli & Jarvenpaa 2000). Each participant's actual performance score was computed as the percentage of correct decisions.

Participants were rewarded based on their performance scores either in cash (gift card) or course credits (per each participant's expressed preference). Cash payment involved $10 for participation plus up to an additional $20 based on the subject's decision performance. The extra credit involved 0.5% extra credit plus up to 1% additional extra credit based on the subject's decision performance. The additional amount of cash or extra credit earned was directly proportional to the participants' actual performance. Of 865 participants, 701 (81%) chose extra credit and 164 (19%) chose cash payment. We carried out a t-test for the mean difference between the performance scores of subjects based on the two types of incentives. The t-test was not statistically significant. Therefore, the data from both groups were combined and used in the analysis.

The protocol involved three stages. In Stage 1, prior to the experiment, the participants answered questions regarding their past experience, their profiles, and other pre-experiment questions. Stage 2 involved the experiment during which data on participants' actions and decisions were collected. At Stage 3, after the completion of the experiment, the participants continued with the online survey to answer manipulation check questions, their familiarity with the domain and with the assigned websites in the experiment, and remaining perceptual questions in the instrument. The experiment was controlled by an extensive software tool specifically designed and implemented for this study. It was written in Java and was administered via the local area network in order to protect the computer systems from potential threats caused by visiting the concocted and spoofed websites. The experiment lasted about 50 minutes.

4.2. Scale Development

Whenever possible, the measurement scales for the constructs in the DTI model were adopted from literature and modified for the current study. All items were converted to semantic differential scales to ensure content validity and to reduce of the threat of common method variance (Chin, Johnson, & Schwarz, 2008; Podsakoff, MacKenzie, & Lee, 2003). Table 2 reports the construct definitions and major sources for scale development, and Appendix A contains the details of the instrument. The measurement items for perceived threat susceptibility, perceived threat severity, user perceived response efficacy, and perceived self-efficacy in taking countermeasures to deal with fake websites were adapted from Witte et al. (1996). The items for reported reliance on the detector were adapted from Davis (1989), Straub et al. (1995) and Venkatesh et al. (2003). The items for cost of detector error were developed for this study. User perceptions regarding the detector's accuracy and speed were measured by a single item.

All the scales for the profile variables were also adopted from literature and modified for this study. The items for the security habit were adapted from Pavlou and Fygenson (2006). The items for past encounters with fake websites were adapted from Chen and Zahedi (2009). Gender, age, and education were measured by a one-item scale. Familiarity with the domain and familiarity with each website were measured by one item developed for this study. As previously alluded to, actual user performance was measured objectively by assessing participants' decisions.

4.3. Pretest, Pilot Test, and Data Collection

The experiment protocol and the instrument were pretested and pilot-tested as recommended by the literature (Boudreau, Gefen, & Straub, 2001; Straub, 1989). All the construct items, the experiment protocol, and experiment instructions were pretested with two faculty members and two PhD students. Based on their feedback, we refined the constructs and clarified the wording of the survey instruments and the experiment instructions. A faculty and a PhD student pretested the experiment protocol, process, and timing. Pilot tests involved two sets. For the online-pharmacies domain, the experiment was pilot tested with 28 participants. For the online-banks domain, there were two rounds of pilot tests, involving 6 and 26 participants, respectively. Pilot-test participants were recruited from the campus of a Midwestern university.

After completing each pilot test, the participants were asked to respond to a set of open-ended questions regarding the clarity and timing of the experiment and instructions as well as the questions in the survey instrument. The survey instrument, experiment procedure and instructions were modified based on the pilot tests. Using the pilot data, we conducted initial manipulation checks and found all manipulations to be successful.

Eight hundred and sixty-five participants from students and staff in a large Midwestern university participated in the experiment—437 participated in the online-pharmacies domain, and 428 participated in the online-banks domain. Table 3 reports the profile information for the two domains.

Table 3. Participant Profiles

Profile variables	Mean			STD		
	Pharm (n = 437)	Bank (n = 428)	Pooled (n = 865)	Pharm (n = 437)	Bank (n = 428)	Pooled (n = 865)
Age	22.4	20.5	21.5	5.6	4.0	4.9
Education*	3.2	3.0	3.1	0.9	0.8	0.9
Hours spent daily on the Internet	3.7	3.6	3.7	1.1	1.0	1.0
Gender	**Male (%)**			**Female (%)**		
	64.3%	60.0%	62.2%	35.7%	40.0%	37.8%

* Education scales, 1 = Some school, no degree, 2 = High school graduate, 3 = Some college, no degree/college students, 4 = Professional degree/2-year associate degree, 5 = Bachelor's degree, 6 = Master's degree, 7 = Doctoral degree.

5. Analysis and Results

5.1. Manipulation and Saliency Checks

In the post-experiment survey, participants were asked to assess the detector's run time speed, accuracy and the cost of making one wrong decision based on what they had experienced in the experiment, which we had manipulated during the experiment. Table 4 reports the results of three ANOVA tests for the two samples as well as the pooled sample.

The results supported the success of manipulation. Furthermore, regression analyses of response efficacy, coping self-efficacy, effort requirement, and loss due to detector error with the corresponding tool elements (accuracy, speed, and cost of error) had statistically significant coefficients in all the three samples (pharmacies, banks, and pooled). This indicated that participants formed their perceptions of tool elements based on the manipulated values of these elements.

Table 4. Manipulation Checks for Tool Elements

Manipulation	Assessment question[a]		Means (STD)		F-Value (d.f.)	Sig. diff.
			Level 1	Level 2		
Detection time (1 vs. 4 seconds)	The detection time of the tool was:	Ph[b]	1.84 (1.82)	4.11 (1.24)	223.08*** (1, 418)	Yes
		Bk	2.08 (2.12)	4.39 (1.47)	170.67*** (1, 426)	Yes
		Pl	1.96 (1.98)	4.25 (1.37)	383.48*** (1,846)	Yes
Detection accuracy (60% vs. 90%)	The tool accuracy was:	Ph	0.57 (0.16)	0.73 (0.23)	70.32*** (1, 415)	Yes
		Bk	0.59 (0.17)	0.77 (0.20)	105.15*** (1, 426)	Yes
		Pl	0.59 (0.16)	0.75 (0.20)	172.18*** (1, 843)	Yes
Cost per wrong decision ($1 vs. $10)	The cost of making one wrong decision was:	Ph	2.64 (3.29)	9.81(1.65)	807.37*** (1,423)	Yes
		Bk	2.75 (3.14)	9.87 (1.60)	873.81*** (1,426)	Yes
		Pl	2.69 (3.21)	9.84 (1.62)	1682.18*** (1, 851)	Yes

[a] The lead part of those assessment questions is "When it comes to some features of the tool you just experienced in the experiment"; [b] Ph = pharmacy (n = 437), Bk = bank (n = 428), and Pl = pooled (n = 865); *** p<0.001.

5.2. Validity and Reliability Checks

We carried out exploratory factor analyses (EFA) to check the convergent and discriminant validity of the constructs in the pharmacies and banks samples, as recommended by the literature (Anderson & Gerbing, 1982; Moore & Benbasat, 1991; Straub, Boudreau, & Gefen, 2004). All measurement items correctly loaded on the corresponding constructs. Appendix B reports all item loadings are greater than 0.70, and no cross loadings are greater than 0.40 (McKnight et al., 2002). Therefore, the convergent and discriminant validities of the constructs were supported.

Table 5 reports the results of reliability checks. Cronbach alpha values were greater than the cutoff value of 0.70 (Nunnally, 1978), and composite factor reliability (CFR) values were above the threshold of 0.70 (Segars 1997). The average variance extracted (AVE) values were above the cutoff value of 0.50 (Segars, 1997). Hence, the reliability checks support the reliability of the constructs.

Table 5. Construct Reliability Checks

Constructs	Pharmacy			Bank		
	Cronbach's α	CFR	AVE	Cronbach's α	CFR	AVE
Detector response efficacy	.97	.97	.91	.97	.97	.92
Coping self-efficacy	.93	.93	.81	.93	.93	.81
Threat severity	.93	.93	.81	.93	.93	.82
Threat susceptibility	.94	.94	.83	.94	.94	.84
Reliance on the detector	.94	.94	.84	.94	.94	.85
Cost of error	.87	.87	.69	.86	.86	.68

By comparing the square root of the AVE for each construct with its correlations with all other constructs, we checked for further evidence of the discriminant validity of the constructs. The square root of AVE for each construct was greater than the correlation values with other constructs (Table 6), further supporting the discriminant validity of the constructs (Fornell & Larcker, 1981).

Table 6. Construct Correlations and Comparison with Square Root of AVEs						
Constructs (Pharmacy)	**1**	**2**	**3**	**4**	**5**	**6**
1. Threat susceptibility	**0.91** [a]					
2. Threat severity	0.28	**0.90**				
3. Reliance on the detector	0.05	0.03	**0.92**			
4. Cost of error	0.15	0.10	-0.05	**0.94**		
5. Detector response efficacy	-0.01	-0.03	0.53	-0.21	**0.83**	
6. Coping self-efficacy	-0.01	0.02	0.21	-0.31	0.25	**0.90**
Constructs (Bank)	**1**	**2**	**3**	**4**	**5**	**6**
1. Threat susceptibility	**0.92**					
2. Threat severity	0.16	**0.91**				
3. Reliance on the detector	0.04	0.15	**0.92**			
4. Cost of error	-0.02	0.22	-0.07	**0.82**		
5. Detector response efficacy	0.01	0.14	0.48	-0.33	**0.96**	
6. Coping self-efficacy	0.04	0.02	0.14	-0.40	0.34	**0.90**
[a] The square root values of the AVEs are highlighted on the diagonal.						

To minimize common method variance (CMV), as suggested by Podsakoff et al. (2003), we used semantic differential scales in the instrument to increase the proximal and methodological separation and to reduce "acquiescence bias" caused by respondents' possible tendency to provide socially desirable answers and/or to agree with the researcher (Chin et al., 2008).

Furthermore, we collected data in multiple stages of the experiment (before, during, and after the experiment), hence creating time intervals between the collection the perceptual data. After data collection, we conducted the exploratory factor analysis. As Appendix B reports, no single factor emerged as a dominant factor, and multiple factors emerged with eigenvalues greater than one. We then conducted Harman's single-factor test (Podsakoff et al., 2003) to further test for the presence of CMV. We found that the single factor accounted for 17.0 percent, 18.8 percent, and 17.7 percent of the variances of the online-pharmacies sample, online-banks sample, and pooled sample, respectively, which were desirably below the 20 percent threshold used in the literature (Igbaria, Zinatelli, Cragg, & Cavaye, 1997; Song & Zahedi, 2005). However, to further minimize any potential threat of common method variance, we used the data of a marker variable (specifically collected for this purpose) to purify our data; thus, the CMV was factored out (Bagozzi, 2011; Podsakoff et al., 2003; Song & Zahedi, 2005). We purified our data by regressing each item on the marker variable and using the regression residuals for data analysis. This process factors out common method bias from the data (Podsakoff et al. 2003). We used the purified data in the analysis.

5.3. Measurement Model

The measurement model was estimated by using the mean-adjusted maximum likelihood (MLM) method in MPlus, which adjusts for non-normality in data. Per Table 7, all fit indices of the measurement model were better than recommended thresholds, indicating a good fit for the measurement model.

Table 7. Measurement Model and DTI Model Fit Indexes			
Fit index	**Measurement model**	**DTI model**	**Threshold***
Normed $\chi 2$	1.41	1.85	<3.0
CFI (comparative fit index)	0.991	0.960	>0.90
TLI (Tucker-Lewis index)	0.990	0.957	>0.90
RMSEA (root mean square error of approximation	0.031	0.044	<0.06
SRMR (standardized root mean square residual)	0.029	0.086	<0.10
*Based on Bentler (1992), Bentler & Bonnett (1980), Browne & Cudeck (1993), Hu & Bentler (1999)			

Confirmatory factor analysis (see Appendix C) shows that the standardized factor loadings of all factors were greater than 0.70, which is satisfactory (Bagozzi, 2011). Moreover, all t-values for the factor loadings were well above the 2.54 cut-off value (Muthén & Muthén, 2003). The high and statistically significant R^2 values, ranging from 0.54 to 0.94 for the pharmacies sample and 0.53 to 0.95 for the banks sample, indicated that the items were appropriate for measuring the corresponding constructs (Gefen, Straub, & Boudreau, 2000).

5.4. Model Estimation

We used the group analysis approach with MLM algorithm in MPlus to estimate the DTI model with two groups: online pharmacies and online banks. Per Table 7, all the fit indices of the DTI model were better than the recommended thresholds, indicating good model fit and supporting our theoretical model in both online pharmacies and online banks domains. Figure 2 reports the path coefficients, p-values for one-tailed t-statistic tests, and R^2 values of the estimation for the DTI model for both the online-pharmacies domain (the top values in Figure 2) and the online-banks domain (the bottom values in Figure 2). Significant control variables are reported in Figure 4.

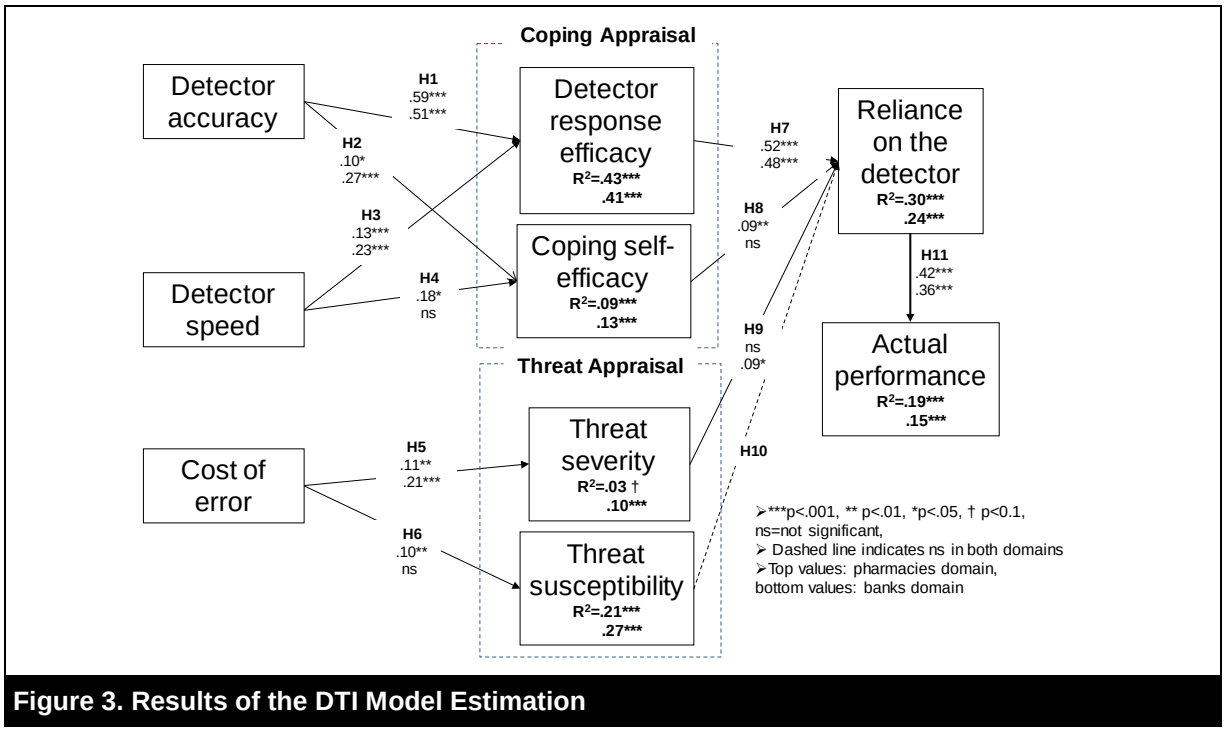

Figure 3. Results of the DTI Model Estimation

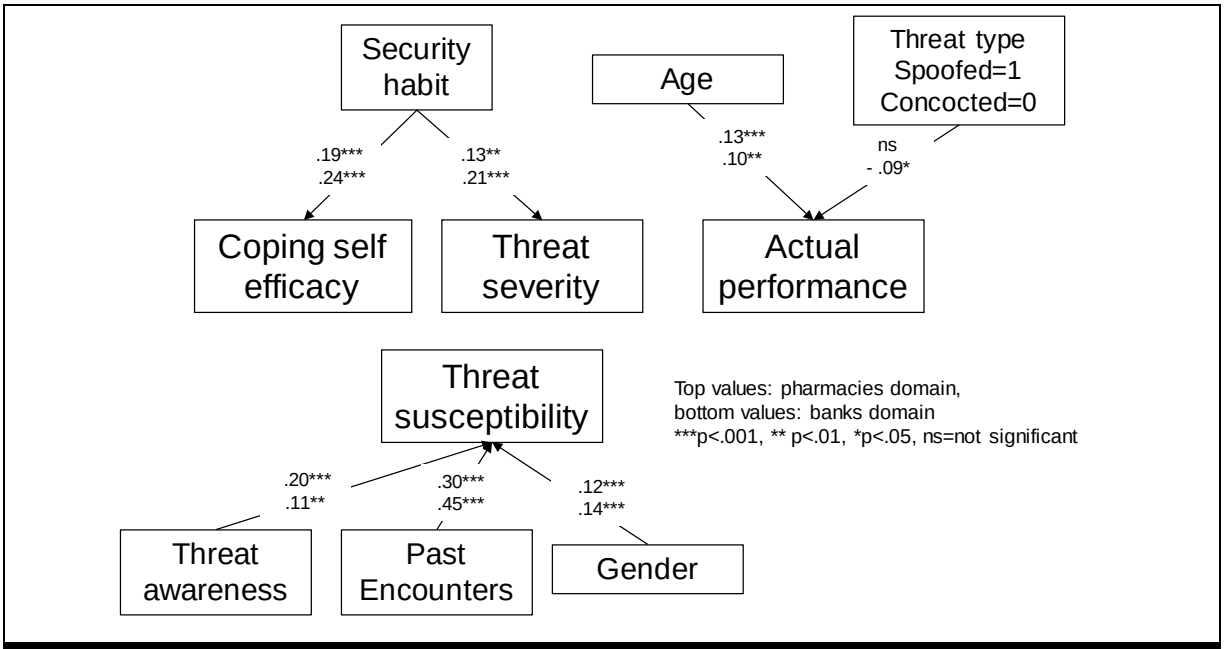

Figure 4. Results for Control Variables in the DTI Model

The R^2 values of all endogenous variables in the model were statistically significant, which demonstrates that the model has reasonable explanatory power.

5.4.1. Hypothesized Paths

Of the 11 hypothesized paths in the DTI model, 10 were statistically significant at least in one of the two domains (Figure 2). H1 and H2 were related to the influence of detector accuracy on detector response efficacy and coping self-efficacy. The results supported H1 and H2 in the two domains, indicating the importance of detector accuracy in coping appraisal. The impact of detector speed on the perception about detector response efficacy and coping self-efficacy were hypothesized in H3 and H4, respectively. The results provided full support for H3 in both domains and for H4 in the pharmacies domain.

The high and significant R^2 values for detector response efficacy for both domains (0.43 and 0.41, $p<0.001$) attest to the explanatory power of tool performance in forming users' perceptions regarding detector response efficacy. R^2 values for coping self-efficacy were also significant in both domains (0.09 and 0.13, $p<0.001$), but at a lower level, indicating the existence of other factors in forming users' coping self-efficacy.

The influence of cost of detector error on threat severity and threat susceptibility was hypothesized in H5 and H6, respectively. Comparing the path coefficients in the two domains for H5 shows that cost of error had significant impact on perceived threat severity in both domains. Its influence was twice as large in the banks domain as in the pharmacies domain. For H6, cost of error had significant impact on threat susceptibility in the pharmacies domain but not in the banks domain, indicating that cost of error in the banks domain had its greatest impact on threat severity. This makes sense since cost of error in online banks has more immediate financial implications. Hence, detection error is perceived to cause more severe financial consequences.

Hypotheses H7-H8 posited that coping appraisal constructs (detector response efficacy and coping self-efficacy) impact the reported reliance on the detector. The results showed that detector response efficacy (H7) was the primary motivator for reliance on the detector in both domains with almost equally high path coefficients. This is in line with findings of Floyd, Prentice-Dunn, and Rogers (2000) that coping variables are stronger behavior motivators than threat variables, and the report by Milne et al. (2000) that "threat appraisal is a poor predictor of intention and behaviors" (p. 134). Coping self-efficacy (H8) was significant for only online banks. The result showed that the secondary motivator of detector use depends on domain.

In online pharmacies where the threat is less severe in terms of direct financial loss, coping self-efficacy acts as the secondary motivator of reliance on the detector, whereas in online banks with immediate financial consequences, threat severity is a stronger motivator of reliance on the detector.

H9 and H10 posited that threat appraisal constructs (threat severity and threat susceptibility) are the antecedents of the reported reliance on the detector. The path for H10 was not significant in either domain, which indicated threat susceptibility had little role in reliance on the detector. However, threat severity was significant in the banks domain, indicating that when the threat involves direct financial consequences, threat severity motivates individuals to heed the detector's advice when visiting financial websites. The statistically significant R^2 values of reliance on the detector in both domains (0.30 and 0.24, $p<0.001$) indicate that the extent of reliance of the detector could be significantly explained by its hypothesized antecedents in the model.

H11 posited that reliance on the detector improves users' actual performance in terms of self-protection against-fake website attacks by avoiding visiting and transacting with fake websites. This hypothesis was strongly supported with high path coefficient values for both domains. Considering the fact that performance was objectively measured, the statistically significant R^2 values of 0.19 and 0.15 for the two domains show that the improvement in individuals' security protection is noteworthy.

5.4.2. Control Variables

For the sake of clarity, we report the significant impacts of control variables in Figure 4. The context-sensitivity in terms of threat type was used as a control since we argued that it influences users' self-protection performance. The results showed that threat type had significant impact on user performance in the online banks domain, but not in the online pharmacies domain. This is a novel finding, indicating that in certain domains with direct financial consequences, the threat of spoofed fake websites could reduce users' efforts in self-protection more than that of concocted websites. We also found that users' self-protection performance improved with age since age had equally significant path coefficients in both domains. It seems that the combination of spoofed threat type and younger age (with less experience or focus) could significantly increase users' vulnerabilities.

The impacts of security habit on coping self-efficacy and threat severity were significant in both domains. The differential influence of security habit was stark in the case of threat severity, where the path coefficient value was 60 percent higher in the banks domain, indicating the importance of security habit in the perception of threat severity.

Several control variables had significant impacts on threat susceptibility. Threat awareness, past encounters with fake-websites, and gender had significant influence on threat susceptibility in both domains. The high significance of threat awareness and past encounters with fake websites show that personal knowledge and experience played a major role in the perception of susceptibility to security threat. Furthermore, women felt more susceptible to threats than men in both domains with almost identical path coefficients. This finding is in line with other IT-related studies indicating gender differences in dealing with IT and risky conditions (e.g., Leonard & Cronan, 2001, Venkatesh et al. 2003). Education was not significant as a control variable. Together, these results indicate that users' profiles have significant influence on their perceptions of security-related constructs, which, in turn, impact their reliance on detection tools and their threat-prevention performance.

5.4.3. Context-Sensitivity with Respect to Domain Type

H12 posited that domain moderates the paths in the DTI model. We conducted the pairwise t-test of path coefficients, using pooled standard errors to test for context-sensitivity (Table 8).

Table 8. Pairwise T-Test of Domain Differences

Antecedent and consequent paths	Path coefficient		Pairwise t-test
	Pharmacy	Bank	
Detector response efficacy			
H1: Detector accuracy→Response efficacy	0.59***	0.51***	ns
H3: Detector speed→Response efficacy	0.13***	0.23***	†
H7: Response efficacy →Reliance on the detector	0.52***	0.48***	ns
Coping self-efficacy			
H2: Detector accuracy→ Coping self-efficacy	0.10*	0.27***	**
H4: Detector speed→Coping self-efficacy	0.18*	ns	** & st
H8: Self-efficacy→Reliance on the detector	0.09**	ns	* & st
Threat severity			
H5: Cost of error→Severity	0.11**	0.21***	†
H9: Severity→Reliance on the detector	ns	0.09*	* & st
Threat susceptibility			
H6: Cost of error→Susceptibility	0.10**	ns	* & st
H10: Susceptibility→Reliance on the detector	ns	ns	ns
Reliance on the detector			
H11: Reliance on the detector→Actual performance	0.42***	0.36***	ns

***p<.001, ** p<.01, *p<.05, †p<0.1, ns = not significant, st = structurally different (one path is significant and the other is insignificant).

The results showed that domain did not play a significant moderating role in the paths from detector performance (accuracy and speed) to reliance on the detector, except for a directional influence of speed on response efficacy. In other words, the paths (detector performance→response efficacy→user reliance) were statistically and strongly significant in both domains and were not sensitive to the two domain types. However, paths from detector performance to user reliance (H2, H4, and H8) were significantly sensitive to the type of domain. This indicates that context-sensitivity of domain type exerts its moderating influence on the paths from detector performance to users' reliance on the detector via coping self-efficacy.

The results also indicated the presence of context-sensitivity in paths from cost of detector error to user reliance via threat perceptions (severity and susceptibility). The paths cost of error → severity → user reliance exhibited statistically significant context-sensitivity, although the path cost of error → severity was marginally significant. The path cost of error → susceptibility also showed significant context-sensitivity. Finally, the path from user reliance on users' actual performance in self-protection did not exhibit significant context-sensitivity.

6. Discussion

In this study we examined the influence of benefit and cost of detection tools in promoting users' reliance on such tools and their actual self-protection performance; and whether context-sensitivity has any role in this process. We relied on the core constructs of the protection motivation theory (PMT) and contextualized it to develop the DTI theory, thus extending PMT through the introduction of "context-specificity" and "context-sensitivity."

We identified the candidate salient tool elements based on theory and empirical research in the literature and conceptualized the model using the DTI theory. Based on an elaborate and extensive experimental design, we explored how manipulated perceptions of users with respect to performance-related elements of detection tools, cost of detection error and contextual factors impact users' threat

appraisal and coping appraisal. We also investigated the consequent impacts of such perceptions on the extent of reliance on detection tools and users' actual performance in self-protection.

First, detector performance, in terms of accuracy and speed, showed a profound influence on user reliance on the detector via the coping appraisal constructs. Moreover, detector response efficacy as a coping mechanism emerged as the single pivotal factor linking detection tools' performance to users' reliance on such tools and subsequently to users' actual performance in self-protection. The sheer dominance of response efficacy is a novel finding for creating and promoting fake-website detection tools. People generally are not good at detecting deceptions (Biros et al., 2002; DePaulo et al., 1985). Hence, a great deal of effort is allocated to increasing accuracy and reducing the run time of such tools (Abbasi & Chen, 2009a). Our results shed light on the importance of such research and indicate that detection tools should be developed, assessed, and marketed based on these performance criteria. Furthermore, we found that path coefficients linking performance elements and reliance via response efficacy are not context sensitive. This lack of context-sensitivity points to the broadly generalizable importance of the role of perceptions about tools' response efficacy in promoting users' reliance and self-protection performance.

Second, most IS studies treat self-efficacy as an exogenous variable and do not examine forces contributing to its change. Our work showed that detector's performance increases users' coping self-efficacy. This is a novel finding since it indicates that users make a connection between the "ability" of an IT artifact and their own ability. The detector accuracy and to some degree its speed enhance users' perception about their own ability to fight against online security threats. Prior research has shown that users feel better about themselves and their capabilities when using more powerful decision making aids (Hung, 2003). In the context of security behavior research, this finding shows that the detector has the potential to merge with users' ego and to become part of their self-perception—"I have more ability since I have a more powerful tool" (in terms of its accuracy and speed in detecting and preventing the threat).

Third, another major finding in this research is the strong and significant context-sensitivity in the paths from detector performance to users' reliance on the detector via coping self-efficacy. This finding indicates that detectors' accuracy has a strong impact on users' coping self-efficacy in the online banking domain. Thus, users' self-empowerment requires developing and marketing tools that boast a high accuracy rate in financially sensitive domains. However, coping self-efficacy does not promote reliance in such domains. Our result suggests that when it comes to financially sensitive domains, such as online banks, it is response efficacy of the detector that prompts users to rely on them. Their own coping self-efficacy counts little in this process. This could be the consequence of familiarity with the domain. Subjects in the online bank domain were twice as familiar with the domain as those in the online-pharmacies domain (with t-test significance of $p<0.001$). It is possible that the influence of self-efficacy on reliance on the detector is not only moderated by the domain but also by the extent of familiarity with the domain. This is a line of research that needs further investigation.

Together, these findings regarding self-efficacy point to the potential for a new theoretical framework in perceiving protective IT artifacts as the extension of self in dealing with online threats. As such, designers of protective IT artifacts must pay closer attention to the psychology of users for whom the tools are being designed and domains in which they are used, thus highlighting the need for protective IT artifacts that have intelligence and can be personalized.

Fourth, another major finding in this work is the strong and significant role of user reliance on the detector in objectively assessed user performance in self-protection against fake-website threats. While implied anecdotally in prior studies (Wu et al., 2006; Dhamija et al., 2006), we believe our result is the first to establish that users' reliance on the detector has significant impact with high path coefficient values on users' performance in multiple contexts. The fact that the path coefficients were almost equally high in both online-pharmacy and online-bank domains shows that, by relying on the detector, users significantly improve their success in avoiding fake-website threats regardless of the domain type.

Fifth, the impact of cost of detector error on users' threat appraisal was context sensitive. Cost of detector error had much larger impact on the perception of threat severity, which, in turn, significantly influenced reported reliance in the online-banks domain, whereas it had no significant impact in the online-pharmacies domain. Losses attributable to fake online banks were perceived as more consequential than losses attributable to purchasing drugs from fake online pharmacies, possibly due to the fact that our sample was comprised of younger subjects.

However, cost of detector error had little influence on users' perception of threat susceptibility. We observed its significant impact on threat susceptibility only in the online-pharmacies domain. Furthermore, threat susceptibility as a mediator of cost of detector error on user reliance had no support in either of the two domains.

Sixth, we examined context-sensitivity with respect to threat type. We argued that, due to the lack of users' awareness of threat type, it influences only their self-protection performance. Hence, we examined its role as a control variable. The results supported this argument, indicating that users' performance deteriorates when the threat goes from concocted to spoofed fake website. This makes sense since spoofed fake websites imitate familiar and well-known websites, which makes it harder for users to detect the deception. We also found that age has a positive influence on user performance. It seems that there is a need to educate younger users regarding the threat of fake-website attacks, particularly about spoofed attacks.

Seventh, the significant roles of security habit, threat awareness, and past encounters with fake websites indicate that users' knowledge, experience and habit are salient in their security behaviors and performance. Moreover, the significance of gender shows that women feel more susceptible. Together, these results indicate the need to take into account the users' personal profiles in developing protective tools and the need for an intelligent approach to the design of detection tools.

7. Implications, Limitations, and Future Directions

7.1. Theoretical Implications

This paper makes a number of novel contributions to theory. Following the theory development arguments by Hong et al. (2014), Johns (2006), Whetten et al. (2009), and Whetten (2009), we borrowed and extended the protection motivation theory (PMT) by contextualizing it—introducing "context specificity" and investigating its "context sensitivity." This led to the detection tool impact (DTI) theory. The DTI theory's "context specificity" involved core antecedent variables (in terms of detector benefit and cost) and outcome variables (in terms of users' reliance on the detector and users' actual self-protection performance). We examined the theory's context-sensitivity by investigating the role of domain type and threat type. The contextualized DTI theory is a novel theoretical contribution of this work, which opens a new avenue for its extension and elaboration to other types of security tool.

Second, this study found that accuracy and speed of the detector and perceived detector response efficacy are the most important factors in users' utilization of detection tools to counter online deceptions. Our work shows that the intellectual investment in improving accuracy and speed is indeed a worthwhile endeavor that should be used in publicizing the performance of detection tools.

Third, our work is the first to show the strong link between the reported reliance on detection tools and users' actual performance in avoiding fake-website attacks. It shows the critical paths of detector performance→detector response efficacy→reliance on the detector→user self-protection performance in two domains. Although the paths look intuitive, there is little evidence in the literature in conceptualizing and scientifically testing their significance. Such evidence is needed in order to convince internet users that the extra effort involved in using detection tools actually pays off in protecting them against fake-website attacks.

Fourth, our findings uncovered the ways to enhance users' coping self-efficacy through suitable development of detection tools. Our findings show that users may view protective IT artifacts as an

extension of their selves, thus reinforcing the need to combine the design science approach with behavioral theories to fit protective IT artifacts to individuals' psychology in order to promote their use. Reinforcing this ego-boosting perspective of protective tools is the role of self-efficacy, which can be enhanced through performance elements of tools, leading to users' reliance on the detector as moderated by domain type. This is a novel finding that opens a new avenue of research into self-efficacy's role in dealing with security threats and the design of intelligent tools with personalization capabilities.

Finally, this study contributes to design science research by proposing and empirically testing the DTI model by which design science scholars can test and evaluate various salient elements of protective IT artifacts. Given the differences in the theoretical foundation for adoption behaviors and for avoidance behaviors (Liang & Xue, 2009), the DTI model may be a more suitable and specialized alternative to the technology acceptance model as an evaluation model for protective IT artifacts.

7.2. Practical Implications

This study provides a framework for the empirical design and evaluation of protective IT artifacts. By manipulating performance and context elements under this framework, designers can test and evaluate the usability and effectiveness of various design prototypes of a protective IT artifact. The implications for practice are far-reaching. First, based on the findings of this study, to increase adoption of a protective IT artifact, designers need to focus on users' coping appraisal process. Second, perceived response efficacy could be used as a metric for evaluating designs of protective tools, assessing their performance, and promoting their use. This provides a clear and consistent strategy for security software and Web browser development companies that produce such tools. Although satisfaction has emerged as a perceptual construct to gauge customers' behaviors, users' perceived response efficacy as a metric of users' behavior and perception has not received adequate recognition. Our results underline the importance of this metric for measuring users' perceptions and behaviors.

Third, the findings show that tool developers should strive for maximum accuracy and speed in application domains. Fake-website detection tool developers routinely balance two competing considerations: accuracy versus runtime. Research has shown that tools that incorporate a larger, more sophisticated set of signatures (i.e., "fraud cues") are capable of detecting fake websites with greater accuracy but at the expense of longer runtimes; in some cases, several seconds longer per detection (Abbasi & Chen, 2009b). Interestingly, in our study, users showed a clear preference for "having the cake and eating it too," with more accurate, faster detection garnering the highest response efficacy.

Fourth, software companies that produce detectors should pay special attention to the potential market for intelligent tools that can be personalized based on the domain of websites as well as on users' traffic patterns and profiles. Personalization could increase the efficacy of detectors and people's interest in using them. Personalized intelligent detectors could be either free standing tools or integrated with intelligent assistants on which users rely for various personal tasks.

Finally, our findings suggest that increasing reliance on detection tools might be accomplished through positively promoting individuals' coping appraisal. Protective tools are normally promoted by highlighting risk, susceptibility and negative consequences of exposure to threats. Our work shows that organizations and companies with the mandate of promoting security tools may also find value in leveraging positive campaigns that increase public awareness of the accuracies and runtime speeds associated with protective tools. The collective reliance on such tools could reduce the success of fake websites and increase online security.

7.3. Limitations and Future Research

This study has limitations. We collected our data for two sensitive domains—online pharmacies and online banks. Therefore, our results should be interpreted within these domains. In addition, our participants interacted with detection tool stimuli that were not embedded in an Internet browser or running as a real-time system. This could be considered a limitation. However, our stimuli closely imitated main features of existing detection tools while eliminating brand name bias. Thus, participants had a unified experiment platform and, consequently, variances due to participants'

varying experiences and knowledge of specific tools were removed. Further, this study was conducted within an academic environment, mostly with younger undergraduate and graduate students. Although such a population represents a large proportion of Internet users, care must be taken in generalizing our findings to other populations such of those in other countries and older adults. However, it is important to note that fake websites are a pertinent problem for the population segment utilized in this study. The two most commonly targeted groups for fake-website attacks are students and the elderly (Ramzan & Wuest, 2007). In the context of online banking, younger people (between 18 and 34) are major users of online banking and are also susceptible to online banking-related security threats (McAfee, 2011a). In the context of online pharmacies, 25 percent to 30 percent of people under the age of 35 take at least one prescription drug, and well over 40 percent take over-the-counter medication (Maris, 2012; Center for Disease Control, 2010). Moreover, younger people and students are just as likely to use online pharmacies as other segments of the population (Orizio, Merla, Schulz, & Gelatti, 2011). Therefore, we believe that using a student population to study fake-website detection security behavior in the online banking and online pharmacy domains is warranted. However, future research should also be conducted on older and non-student populations. For instance, as alluded to earlier, it would be interesting to see how these other populations perceive losses in different domains such as online banking and online pharmacies.

This paper has proposed a number of research avenues for building theories that combine the strength of design science and behavioral science in creating compelling personalized protective IT artifacts. Another direction of future research is the use of the DTI theory and model in examining the salient elements for other protective IT artifacts. In situations where a tool may provide detection capabilities for several threats with varying levels of accuracy and speed, it remains unclear how response efficacy for individual tool components (as well as the tool as a whole) would be impacted. Further research investigating salient elements for such enterprise-level security tools with several protective capabilities including fake-website detection, anti-virus, malware protection, intrusion detection, and so on, is warranted. Finally, other Internet usage domains—particularly hedonic domains such as online games and social networking—could be explored in future research. It is possible that the impacts of the detector's salient elements in hedonic domains will be different from those in utilitarian domains such as the online pharmacies and online banks employed in this study.

This paper is part of a larger, federally funded project that involves investigating fake-website detection tools in terms of performance-related elements, user-interface elements, multiple domains, and personalization through intelligent user interface.

Acknowledgements

This work was funded by a grant from the U.S. National Science Foundation: CNS-1049497.

References

Abbasi, A., & Chen, H. (2009a). A comparison of tools for detecting fake websites. *IEEE Computer, 42*(10), 78-86.

Abbasi, A., & Chen, H. (2009b). A comparison of fraud cues and classification methods for fake escrow website detection. *Information Technology and Management*, *10*(2), 83-101.

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., & Nunamaker, J. F., Jr. (2010). Detecting fake websites: The contribution of statistical learning theory. *MIS Quarterly*, *34*(3), 435-461.

Abbasi, A., Zahedi, F. M., Kaza, S. (2012). Detecting fake medical websites using recursive trust labeling. *ACM Transactions on Information Systems*, *30*(4), 1-36.

Abu-Nimeh, S., Nappa, D., Wang, X., & Nair, S. (2007). A comparison of machine learning techniques for phishing detection. In *Proceedings of the Anti-Phishing Working Groups 2nd Annual Ecrime Researchers Summit* (Pp. 60-69).

Adipat, B., Zhang, D., & Zhou, L. (2011). The effects of tree-view based presentation adaptation on mobile Web browsing. *MIS Quarterly*, *35*(1), 99-122.

Airoldi, E., & Malin, B. (2004). *Data mining challenges for electronic safety: The case of fraudulent intent detection in e-mails*. Paper presented at the Workshop on Privacy and Security Aspects of Data Mining.

Akhawe, D., & Felt, A. P. (2013). Alice in warningland: A large-scale field study of browser security warning effectiveness. In *Proceedings of the 22nd USENIX Security Symposium*.

An, B. (2010). 14 arrested for making, selling fake drugs via bogus military medical websites. *Xinhua Net*. Retrieved from http://big5.xinhuanet.com/gate/big5/news.xinhuanet.com/english2010/china/2010-02/05/c_13165317.htm

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613-643.

Anderson, J., & Gerbing, D. (1982). Some methods for respecifying measurement models to obtain unidimensional construct measurement. *Journal of Marketing Research*, *19*(4), 453-460.

Angst, C. M., & Agarwal R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly*, *33*(2), 339-370.

Armin, J. (2010). Internet drug rings and their "killer" online pharmacies. *Internet Evolution*. Retrieved from http://www.internetevolution.com/author.asp?section_id=717&doc_id=191640

Bagozzi, R. P. (2011). Measurement and meaning in information systems and organizational research: Methodological and philosophical foundations. *MIS Quarterly, 35*(2), 261-292.

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist, 37*(2), 122-147.

Bandura, A. (1997). Self-efficacy: The exercise of control. New York: Macmillan.

Bandura, A., Adams, N. E., & Beyer, J. (1977). Cognitive processes mediating behavioral change. *Journal of Personality and Social Psychology*, *35*(3), 125-139.

Bansal, G. Zahedi, F. M., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, *49*(2), 138-150.

Bansal, G. Zahedi, F. M., & Gefen, D. (2008). The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation. In *Proceedings of 29th International Conference on Information Systems*.

Basagiannis, S., Katsaros, P., Pombortsis, A., & Alexiou, N. (2009). Probabilistic model checking for the quantification of DoS security threats. *Computer and Security*, *28*(6), 450-465.

Bentler, P. M. (1992). On the fit of models to covariances and methodology to the bulletin. *Psychological Bulletin, 112*(3), 400-404.

Bentler. P. M., & Bonnett, D.G. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychological Bulletin, 88*(3), 588-606.

Biros, D. P, George, J. F., & Zmud, R. W. (2002). Inducing sensitivity to deception in order to improve decision making performance: A field study. *MIS Quarterly*, *26*(2), 119-144.

Bliss, J. P., Gilson, R. D., & Deaton, J. E. (1995). Human probability matching behavior in response to alarms of varying reliability. *Ergonomics*, *38*(11), 2300-2312.

Boudreau, M.-C., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: A state-of-the-art assessment. *MIS Quarterly, 25*(1), 1-16.

Bravo-Lillo, C., Cranor, L. F., Downs, J. S., & Komanduri, S. (2011). Bridging the gap in computer security warnings: A mental model approach. *IEEE Security and Privacy*, *9*(2), 18-26.

Browne, M. W., & Cudeck, R. (1993). Alternative ways of assessing model fit. In K. A. Bollen & J. S. Long (Eds.), *Testing structural equation models* (pp. 445-455). Newbury Park, CA: Sage.
Camp, L. J. (2009). Mental models of privacy and security. *IEEE Technology and Society Magazine*, *28*(3), 37-46.
Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. *Information Systems Research*, *16*(1), 28-46.
Center for Disease Control. (2010). *Prescription drug use continues to increase: U.S. prescription drug data for 2007-2008* (NCHS Data Brief No. 42).
Chen, Y., & Zahedi, F. M. (2009). Internet users' security behaviors and trust. In *Proceedings of the Pre-ICIS Workshop on Information Security and Privacy*.
Chen, Y., Zahedi, M., & Abbasi, A. (2011). Interface design elements for anti-phishing systems. In H. Jain, A. P. Sinha, & P. Vitharana (Eds.), *Service-oriented perspectives in design science research* (Vol. 6629, pp. 253-265). Berlin: Springer-Verlag.
Chen, Z., Zhang, X., Leung, K., & Zhou, F. (2010). Exploring the interactive effect of time control and justice perception on job attitudes. *The Journal of Social Psychology*, *150*(2), 181-197.
Chin W.W., Johnson, N., & Schwarz, A. (2008). A fast form approach to measuring technology acceptance and other constructs. *MIS Quarterly*, *32*(4), 687-703.
Chou, N. Ledesma, R., Teraguchi, Y., Boneh, D., & Mitchell, J. C. (2004). Client-side defense against Web-based identity theft. In *Proceedings of the Network and Distributed System Security Symposium.*
Chua, C. E. H., & Wareham, J. (2004). Fighting Internet auction fraud: An assessment and proposal. *IEEE Computer, 37*(10), 31-37.
Cranor, L. F. (2008). A framework for reasoning about the human in the loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security* (pp. 1-15).
Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, *9*(2), 189-211.
Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319-340.
DePaulo, B. M., Stone, J. I., & Lassiter, G. D. (1985). Deceiving and Detecting Deceit. In B. R. Schlenker (Ed.), The self and social life, New York, NY: McGraw-Hill Book Company.
Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In *Proceedings of the ACM Conference on Computer Human Interaction* (pp. 581-590).
Dinev, T. (2006). Why spoofing is serious internet fraud. *Communications of the ACM, 49*(10), 76-82.
Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of AIS, 8*(7), 386-408.
Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. In *Proceedings of the Second Symposium on Usable Privacy and Security* (pp. 79-90).
Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioral response to phishing risk. In *Proceedings of the ACM Anti-Phishing Working Groups 2nd Annual Ecrime Researchers Summit* (pp. 37-44).
Easton, G. (2007). Clicking for pills. *British Medical Journal, 334*(7583), 14-15.
Edworthy, J. (1997). Cognitive compatibility and warning design. *International Journal of Cognitive Ergonomics*, *1*(3), 193-209.
Egelman, S., Cranor, L. F., & Hong, J. (2008). You've been warned: An empirical study of the effectiveness of Web browser phishing warnings. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems* (pp. 1065-1074).
Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407-429.
Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39-50.
Francis-Smythe, J. A., & Robertson, I. T. (2003). The importance of time congruity in the organization. *Applied Psychology*, *52*(2), 298-321.
Gartner. (2011). *Magic quadrant for web fraud detection.*
Gefen, D., Straub, D. W., & Boudreau, M.-C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems, 4*, 1-79.

Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of internet fraud: An empirical investigation of deception and trust with experienced internet consumers. *IEEE Transactions on Systems, Man, and Cybernetics: Part A, 20*(4), 395-410.

Grazioli, S., & Jarvenpaa, S. L. (2003). Consumer and business deception on the Internet: Content analysis of documentary evidence. *International Journal of Electronic Commerce*, *7*(4), 93-118.

Greenberg, A. (2008). *Pharma's black market boom. Forbes.com*.

Gyongyi, Z., & Garcia-Molina, H. (2005). Spam: It's not just for inboxes anymore. *IEEE Computer*, *38*(10), 28-34.

Herzberg, A., & Jbara, A. (2008). Security and identification indicators for browsers against spoofing and phishing attacks. *ACM Transactions on Internet Technology, 8*(4), 1-36.

Hong, W., Chan, F. Y. K., Thong, J. Y. L., Chasalow, L. C., & Dhillon, G. (2014). A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research*, *35*(1), 111-136.

Hu, L., & Bentler, P. M. (1999). Cut-off criteria for fit indexes in covariance matrix analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling, 6*(1), 1-55.

Hung, S. Y. (2003). Expert versus novice use of the executive support systems: An empirical study. *Information and Management, 40*(3), 177-189.

Igbaria, M., Zinatelli, N., Cragg, P., & Cavaye. A. L. M. (1997). Personal computing acceptance factors in small firms: A structural equation model. *MIS Quarterly*, *21*(3), 279-302.

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

Javelin Strategy. (2014). *2014 identity fraud report: Card data breaches and inadequate consumer password habits fuel disturbing fraud trends*. Retrieved from https://www.javelinstrategy.com/brochure/314

Johns, G. (2006). The essential impact of context on organizational behavior. *Academy of Management Review*, *31*(2), 386-408.

Johnson, P. E., Grazioli, S., Jamal, K., & Berryman, G. (2001). Detecting deception: Adversarial problem solving in a low base rate world. *Cognitive Science*, *25*(3), 355-392.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549-566.

Jonsson, I.-M., Harris, H., & Nass, C. (2008). How accurate must an in-car information system be? Consequences of accurate and inaccurate information in cars. In *Proceeding of the 26th Annual SIGCHI Conference on Human Factors in Computing Systems* (pp. 1665-1674).

Kramer, J., Noronha, S., & Vergo, J. (2000). A user-centered design approach to personalization. *Communications of the ACM, 43*(8), 45-48.

Krebs, B. (2005). Few online "Canadian pharmacies" based in Canada, FDA says. *WashingtonPost.com*.

Kumaraguru, P. (2009). *A system for educating users about semantic attacks* (Doctoral Dissertation). Carnegie Mellon University.

Kumaraguru, P., Sheng, S., Aquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology, 10*(2), 1-31.

Li, L., & Helenius, M. (2007). Usability evaluation of anti-phishing toolbars. *Journal in Computer Virology*, *3*(2), 163-184.

Lam, C. Y., & Lee, M. K. O. (2006). Digital inclusiveness—longitudinal study of internet adoption by older adults. *Journal of Management Information Systems, 22*(4), 177-306.

Lau, R. Y. K., Liao, S. Y., Kwok, R. C., Xu, K., Xia, Y., & Li, Y. (2011). Text mining and probabilistic language modeling for online review spam detection. *ACM Transactions on MIS*, *2*(4), 1-25.

Lee, W., Fan, W., Miller, M., Stolfo, S., & Zadok, E. (2002). Toward cost-sensitive modeling for intrusion detection and response. *Journal of Computer Security, 10*(1/2), 5-22.

Lennon, M. (2011). Cisco: Targeted attacks cost organizations $1.29 billion annually. *Security Week*.

Leonard, L. N. K., & Cronan, T. P. (2001). Illegal, inappropriate, and unethical behavior in an information technology context: A study to explain influences. *Journal of the Association for Information Systems*, *1*(12), 1-31.

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

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394-413.

Macan, T. H. (1994). Time management: Test of a process model. *Journal of Applied Psychology*, *79*, 381-391.
Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concern (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336-355.
Maris, D. (2012). Who is popping all those pills? *Forbes Magazine*.
Marks, R., & Allegrante, J. P. (2005). A review and synthesis of research evidence for self-efficacy-enhancing interventions for reducing chronic disability: Implications for health education practice (part II). *Health Promotion Practice*, *6*(2), 148-156.
McAfee. (2011a). *Guide to online banking safety for carefree, confident, and conservative customers*. Retrieved from https://blogs.mcafee.com/consumer/guide-to-online-banking-safety
McAfee. (2011b). *McAfee threats report: Fourth quarter 2010*. Retrieved from http://www.mcafee.com /us/about/news/2011/q1/20110208-01.aspx
McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, *13*(3), 334-359.
Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, *30*(1), 106-143.
Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research, 2*(3), 192-222.
Muthén, B. O., & Muthén, L. (2003). *The comprehensive modeling program for applied researchers user guide.* Los Angeles, CA: Muthén & Muthén.
Nunnally, J. (1978). *Psychometric theory*. New York: McGraw-Hill.
Orizio, G., Merla, A., Schulz, P. J., & Gelatti, U. (2011). Quality of online pharmacies and websites selling prescription drugs: A systematic review. *Journal of Medical Internet Research, 13*(3), e74.
Parasuraman, R., & Miller, C. A. (2004). Trust and etiquette in high-criticality automated systems. *Communications of the ACM, 47*(4), 51-55.
Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly*, *30*(1), 115-143.
Podsakoff, P. M., MacKenzie, S. B., & Lee, J.-Y. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879-903.
Ramzan, Z., & Wuest, C. (2007). Phishing attacks: Analyzing trends in 2006. In *Proceedings of the 4th Conference on Email and Anti-Spam*.
Rice, S. (2009). Examining single- and multiple-process theories of trust in automation. *The Journal of General Psychology*, *136*(3), 303-319.
Rippetoe, P. A., & Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology*, *52*(3), 596-604.
Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, *91*, 93-114.
Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protected motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology: A source book*. New York, NY: The Guilford Press.
Rovira, E., McGarry, K., & Parasuraman, R. (2002). Effects of unreliable automation on decision making in command and control. In *Human Factors and Ergonomics Society Annual Meeting Proceedings* (pp. 428-432).
SAP. (2013). The mobile consumer insights on global trends impacting mobile momentum and customer engagement. Retrieved from http://www.sap.com/pc/tech/mobile /featured/offers/mobile-consumer-behaivor-report.html
Schneier, B. (2000). Semantic network attacks. *Communications of the ACM*, *43*(12), 168.
Segars, A. H. (1997). Assessing the unidimensionality of measurement: A paradigm and illustration within the context of information systems research. *Omega*, *25*(1), 107-121.
Smerecnik, C. M. R., Mesters, I., de Vries, N. K., & de Vries, H. (2009). Alerting the general population to genetic risks: The value of health messages communicating the existence of genetic risk factors for public health promotion. *Health Psychology*, *28*(6), 734-745.
Song, J., & Zahedi, F. M. (2005). A theoretical approach to Web design in e-commerce: A belief reinforcement model. *Management Science*, *51*(8), 1219-1235.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-169.
Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communication of AIS, 13*, 380-426.
Straub, D. W., Limayem, M., & Karahanna E. (1995). Measuring system usage: Implications for IS theory testing. *Management Science*, *41*(8), 1328-1342.
Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, *22*(4), 441-469.
Strecher, V. J., DeVellis, B. M., Becker, M. H., & Rosenstock, I. M. (1986). The role of self-efficacy in achieving health behavior change. *Health Education Quarterly*, *13*(1), 73-91.
Sturges, J. W., & Rogers, R. W. (1996). Preventive health psychology from a developmental perspective: An extension of protection motivation theory. *Health Psychology*, *15*(3), 158-166.
Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., & Cranor, L. F. (2009). Crying wolf: An empirical study of SSL warning effectiveness. In *Proceedings of the 18th USENIX Security Symposium.*
Vance, A., Elie-Dit-Cosaque, C., & Straub, D. W. (2008). Examining trust in information technology artifacts: The effects of system quality and culture. *Journal of Management Information Systems*, *24*(4), 73-100.
Vaughan-Nichols, S. J. (2011). Internet Explorer gains Web browser market share from Firefox. *ZDNet.* Retrieved from http://www.zdnet.com/blog/networking/internet-explorer-gains-web-browser-market-share-from-firefox/743
Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425-478.
Virta, J. L., Jacobson, S. H., & Kobza, J. E. (2003). Analyzing the cost of screening selectee and non-selectee baggage. *Risk Analysis*, *23*(5), 897-907.
Weinstein, N. D. (1988). The precaution adoption process. *Health Psychology*, *7*(4), 355-386.
Whetten, D. A. (2009). An examination of the interface between context and theory applied to the study of Chinese organizations. *Management and Organization Review*, *5*(1), 29-55.
Whetten, D. A., Felin, T., & King, B. G. (2009). The practice of theory borrowing in organizational studies: Current issues and future directions. *Journal of Management, 35*(3), 537-563.
White, R. W., & Horvitz, E. (2009). CyberChondria: Studies of the escalation of medical concerns in Web search. *ACM Transactions on Information Systems, 27*(4), 1-37.
Willis, P. (2009). Fake anti-virus software catches 43 million users' credit cards. *Digital Journal*. Retrieved from www.digitaljournal.com/article/280746
Witte K., Cameron, K. A., McKeon, J. K., & Berkowitz, J. M. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication*, *1*(4), p317-342.
Wu, M., Miller, R. C., & Garfunkel, S. L. (2006). Do security toolbars actually prevent phishing attacks? In *Proceedings of the Conference on Human Factors in Computing Systems* (pp. 601-610).
Xiang, G., Hong, J., Rose, C. P., & Cranor, L. (2011). Cantina+: A feature-rich machine learning framework for detecting phishing web sites. *ACM Transactions on Information and System Security*, *14*(2).
Xiao, B., & Benbasat, I. (2011). Product-related deception in e-commerce: A theoretical perspective. *MIS Quarterly, 35*(1), 169-196.
Yue, W. T., & Çakanyildirim, M. (2007). Intrusion prevention in information systems: Reactive and proactive responses. *Journal of Management Information Systems*, *24*(1), 329-353.
Zahedi, F. M., & Song, J. (2008). Dynamics of trust revision: Using health infomediaries. *Journal of Management Information Systems*, *24*(4), 225-248.
Zhang, Y., Egelman, S., Cranor, L., & Hong, J. (2007). Phinding phish: Evaluating anti-phishing tools. In *Proceedings of the 14th Annual Network and Distributed System Security Symposium*.

Appendices

Appendix A: Instrument

Table A-1. Instrument

Constructs	Code	Items
Detector response efficacy		In evaluating the detection performance of the DS (Detection System) to assist me to successfully avoid fake websites, I believe that, the DS was
	res1*	not helpful at all/very helpful for sure
	res2	not valuable at all/very valuable for sure
	res3	not useful at all/very useful for sure
Cost of detector error		When it comes to the cost of following a wrong recommendation made by the DS, I believe that,
	cost1	the extent of my loss was (very low/very high)
	cost2	The amount of money I lost was (very low/very high)
	cost3	In general, the consequence of errors made by the DS was (not severe at all/very severe for sure)
Coping self-efficacy		When it comes to my ability to take protective actions against fake websites, I believe that
	self1	my knowledge for taking protective actions is (not adequate at all / very adequate for sure)
	self2	my ability to take protective actions is (very low/very high)
	self3	for me, taking protective actions is (very difficult/very easy)
Threat Severity		When it comes to the severity of damage due to using fake websites , I believe that
	sev1	the extent of my potential damages due to using fake websites is (very low/very high)
	sev2	my possible loss due to using fake websites is (very low/very high)
	sev3	for me, the extent of the negative consequences of using fake websites (very low/very high)
Threat Susceptibility		When it comes to the likelihood of encountering fake websites, I believe that
	sus1	the chance of my encountering fake websites is (very low/very high)
	sus2	the likelihood that I would encounter fake websites is (very low/very high)
	sus3	the possibility of my encountering fake websites is (very low/very high)
Reported reliance on the detector	rel1	During the experiment, the extent to which I followed the advice of the DS was (very low/very high)
	rel2	In making my decisions during the experiment, the extent of my reliance on the DS advice was (very low/very high)
	rel3	In informing my opinions about the website in the experiment, the extent of my reliance on the DS advice was (very low/very high)
Threat awareness		When it comes to my awareness of fake websites, I
	awe1	don't know anything about them/ know a lot about them
	awe2	haven't heard about them at all/ have heard a lot about them for sure
	awe3	am not familiar with them at all/ am very familiar with them for sure
Security habit		When using the web, for me, taking security precautions is
	hab1	not in my nature at all/in my nature for sure
	hab2	not routine at all/very routine for sure
	hab3	not habitual at all/very habitual for sure
Past encounters with fake websites	past1	When it comes to my past encounters with fake websites, the number of my encounters has been (very low/very high)
	past2	the number of fake websites I visited has been (very low/very high)
	past3	the frequency of my encounters with fake websites has been (very low/very high)
Perceived detector accuracy	Acc	I believe this accuracy it was: not acceptable at all/was acceptable for sure
Perceived detector speed	speed	I believe that this detection time was: not acceptable at all/was acceptable for sure

Appendix B: Exploratory Factor Analysis

Table B-1. Exploratory Factor Analysis for the DTI Model

Constructs	Items	Pharmacies						Banks					
		1	2	3	4	5	6	1	2	3	4	5	6
Cost of detector error	cost1	-.02	-.04	.07	-.13	.09	**.88**	-.03	.00	-.01	.18	-.14	**.86**
	cost2	-.05	-.04	.09	-.18	.03	**.88**	-.14	-.10	-.02	.06	-.23	**.86**
	cost3	-.19	.05	.01	-.05	.00	**.87**	-.23	.06	.01	.07	-.11	**.84**
Response efficacy	res1	**.91**	.29	.00	.10	-.02	-.12	**.90**	.27	.01	.06	.15	-.15
	res2	**.93**	.25	.01	.10	-.02	-.09	**.92**	.23	.00	.08	.15	-.13
	res3	**.93**	.23	-.01	.12	.00	-.08	**.92**	.23	.01	.06	.15	-.15
Coping self-efficacy	self1	.13	.07	-.04	**.91**	.00	-.14	.13	.05	.04	.01	**.89**	-.22
	self2	.10	.08	.03	**.93**	.03	-.12	.18	.03	.02	.02	**.93**	-.16
	self3	.07	.12	.01	**.91**	-.03	-.10	.09	.08	-.01	.00	**.92**	-.10
Threat susceptibility	sus1	.01	.02	**.93**	-.02	.13	.05	.00	.03	**.93**	.11	.03	-.03
	sus2	.00	.02	**.95**	-.03	.13	.06	-.02	.01	**.96**	.05	.00	-.01
	sus3	.00	.01	**.93**	.05	.13	.06	.04	.01	**.93**	.08	.01	.02
Threat severity	sev1	.00	-.01	.12	.01	**.93**	.03	.08	.03	.08	**.93**	.02	.09
	sev2	-.02	.01	.14	.01	**.94**	.04	.07	.06	.08	**.94**	.01	.13
	sev3	-.01	.05	.12	-.01	**.90**	.06	.02	.10	.09	**.91**	.00	.08
Reported reliance on the detector	rel1	.19	**.89**	-.03	.13	.05	-.03	.19	**.90**	.01	.05	.08	-.04
	rel2	.27	**.92**	.02	.07	.01	.03	.21	**.94**	.02	.06	.06	.02
	rel3	.28	**.91**	.07	.09	.00	-.02	.25	**.91**	.02	.09	.02	-.01
Eigenvalue		4.8	3.5	2.5	1.9	1.8	1.3	5.0	3.4	2.7	2.1	1.5	1.2
Cumulative variance explained (%)		15.7	30.6	45.5	60.1	74.7	87.9	15.5	30.7	45.6	60.4	75.2	88.4

Appendix C: Confirmatory Factor Analysis

Table C-1. Results of Confirmatory Factory Analysis (Purified Data)

Constructs	Items	Pharmacies			Banks		
		Loading	t-value	R2	Loading	t-value	R2
Cost of detector error	cost1	0.81	40.55	0.66	0.81	39.11	0.65
	cost2	0.88	40.29	0.77	0.88	50.07	0.77
	cost3	0.80	34.10	0.63	0.79	32.58	0.62
Detector response efficacy	res1	0.94	108.94	0.89	0.95	101.70	0.90
	res2	0.97	178.83	0.94	0.96	88.58	0.92
	res3	0.96	141.68	0.91	0.96	119.70	0.92
Coping self-efficacy	self1	0.89	53.87	0.78	0.89	54.97	0.79
	self2	0.95	64.93	0.89	0.96	70.98	0.92
	self3	0.87	48.61	0.75	0.86	55.07	0.74
Threat susceptibility	sus1	0.89	56.40	0.80	0.90	58.16	0.81
	sus2	0.95	89.44	0.91	0.96	95.36	0.92
	sus3	0.89	52.46	0.79	0.89	56.93	0.80
Threat severity	sev1	0.90	56.83	0.81	0.91	61.85	0.83
	sev2	0.95	67.81	0.91	0.95	68.31	0.90
	sev3	0.85	41.52	0.72	0.86	43.48	0.74
Reliance on the detector	rel1	0.84	40.20	0.70	0.85	52.18	0.73
	rel2	0.97	126.44	0.93	0.97	140.71	0.95
	rel3	0.94	95.59	0.89	0.93	75.34	0.87
Threat awareness	awa1	0.88	55.75	0.77	0.87	56.23	0.76
	awa2	0.74	27.66	0.54	0.73	32.04	0.53
	awa3	0.93	68.61	0.87	0.91	49.22	0.83
Security habit	hab1	0.88	51.59	0.78	0.90	57.41	0.81
	hab2	0.97	124.44	0.94	0.96	81.15	0.92
	hab3	0.95	111.30	0.90	0.96	142.88	0.92
Past encounters with fake websites	past1	0.80	30.13	0.64	0.84	37.74	0.71
	past2	0.88	39.04	0.77	0.90	42.65	0.81
	past3	0.88	41.52	0.77	0.91	55.93	0.83

About the Authors

Fatemeh Mariam ZAHEDI is a professor and Roger L. Fitzsimonds Distinguished Scholar at the Sheldon B. Lubar School of Business, University of Wisconsin-Milwaukee. She has received her doctoral degree from Indiana University. Her areas of research include design and behavior issues in Web-based IT systems, including trust, privacy, and security. She has served as SE and AE of *MIS Quarterly*, editorial board of *JMIS*, and AE of *ISR*. She has published more than 120 referred papers in premier journals and conferences, including *MIS Quarterly*, *Information Systems Research*, *Journal of Management Information Systems*, *Management Science*, IE*EE Transactions on Software Engineering*, *Operations Research*, *IEEE Transactions on Systems, Man, and Cybernetics*, *IIE Transactions*, and *Review of Economics and Statistics*, and others. She has been the PI of grants funded by NSF and other agencies. She is the author of two books: *Quality Information Systems* and *Intelligent Systems for Business: Expert Systems with Neural Network*. She has received several research, teaching, and best paper awards. Her work has been featured in TV and print media. The list of her publications is available on her Google Scholar profile.

Ahmed ABBASI is an associate professor of information technology and director of the Center for Business Analytics in the McIntire School of Commerce at the University of Virginia. He attained his B.S. and MBA degrees from Virginia Tech, and a Ph.D. from the University of Arizona. He has published more than 50 peer-reviewed articles in top journals and conference proceedings, including MIS Quarterly, Journal of Management Information Systems, ACM Transactions on Information Systems, IEEE Transactions on Knowledge and Data Engineering, and IEEE Intelligent Systems. His projects on Internet fraud, cyber security, and social media analytics have been funded through multiple grants from the National Science Foundation. He received the IBM Faculty Award and AWS Research Grant for his work on big data. He has also received best paper awards from *MIS Quarterly*, the Association for Information Systems, and the Workshop on Information Technologies and Systems. He serves as an associate editor for *Information Systems Research*, *Decision Sciences Journal*, *ACM Transactions on MIS*, and *IEEE Intelligent Systems*. His work has been featured in several media outlets, including the *Wall Street Journal*, the Associated Press, and Fox News.

Yan CHEN is an assistant professor at the College of Business, Auburn University at Montgomery. She received her PhD in MIS from the University of Wisconsin–Milwaukee. Her work has focused on information security, cyber espionage, privacy and e-commerce. Her research has been published in journals including the *Journal of Management Information Systems* and the *Journal of Computer Information Systems*, and a number of refereed conference proceedings.