The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived

RYAN T. WRIGHT AND KENT MARETT

RYAN T. WRIGHT is Assistant Professor in the Department of Technology, Innovation, and Entrepreneurship at the University of San Francisco. He holds a Ph.D. in Business Administration from Washington State University. He also holds an MBA and a B.S. in MIS from the University of Montana. Dr. Wright's research interests include e-commerce, human–computer interaction, and online deception. He is a member of the Joint AIS/ACM Task Force for the Undergraduate Information Systems Model Curriculum (IS 2009). His research has been published in *Communications of the AIS, Group Decision and Negotiation,* and *Journal of Electronic Commerce Research,* among others.

KENT MARETT is Assistant Professor of Business Information Systems at Mississippi State University. He received his Ph.D. in MIS from Florida State University. His research is primarily focused on online deceptive communication, information security, the use of technology by work groups, and human–computer interaction. His research has been published in several leading IS journals.

ABSTRACT: Phishing has been a major problem for information systems managers and users for several years now. In 2008, it was estimated that phishing resulted in close to $50 billion in damages to U.S. consumers and businesses. Even so, research has yet to explore many of the reasons why Internet users continue to be exploited. The goal of this paper is to better understand the behavioral factors that may increase one's susceptibility for complying with a phisher's request for personal information. Using past research on deception detection, a research model was developed to help explain compliant phishing responses. The model was tested using a field study in which each participant received a phishing e-mail asking for sensitive information. It was found that four behavioral factors were influential as to whether the phishing e-mails were answered with sensitive information. The paper concludes by suggesting that the behavioral aspect of susceptible users be integrated into the current tools and materials used in antiphishing efforts.

KEY WORDS AND PHRASES: computer-mediated deception, electronic mail fraud, Internet security, interpersonal deception theory, phishing.

THE INTERNET HAS OPENED UP A WEALTH OF OPPORTUNITIES for individuals and businesses to expand the reach and range of their personal and commercial transactions, but these

Journal of Management Information Systems / Summer 2010, Vol. 27, No. 1, pp. 273–303.

0742–1222 / 2010 $9.50 + 0.00.
DOI 10.2753/MIS0742-1222270111

openings have also created a venue for a number of computer security issues that must be addressed. Investments in security hardware and software are now fundamental parts of a company's information technology (IT) budget. Also, security policies are continually developed and refined to reduce technical vulnerabilities. However, the frequent use of Internet technologies by corporations can also introduce new vulnerabilities. One recent phenomenon that exploits end users' carelessness is *phishing*. Phishing uses obfuscation of both e-mails and Web sites to trick Web users into complying with a request for personal information [5, 27]. The deceitful people behind the scam, the "phishers," are then able to use the personal information for a number of illicit activities, ranging from individual identity theft to the theft of a company's intellectual property. According to some estimates, phishing results in close to $50 billion of damage to U.S. consumers and businesses a year [49, 71]. In 2007, phishing attacks increased and some 3 million adults lost over $3 billion in the 12 months ending in August 2007 [29]. Although some reports indicate that the annual financial damage is not rising dramatically from year to year, the number of reported victims is increasing at a significant rate [35]. Phishing continues to be a very real problem for Web users in all walks of life.

Consistent with the "fishing" homonym, phishing attacks are often described by using a "bait-and-hook" metaphor [70]. The "bait" consists of a mass e-mail submission sent to a large number of random and unsuspecting recipients. The message strongly mimics the look and feel of a legitimate business, including the use of familiar logos and slogans. The e-mail often requests the recipient's aid in correcting a technical problem with his or her user account, ostensibly by confirming or "resupplying" a user ID, a password, a credit card number, or other personal information. The message typically encourages recipients to visit a bogus Web site (the "hook") that is similar in appearance to an actual corporate Web site, except that user-supplied information is not sent to the legitimate company's Web server, but to a server of the phisher's choosing. The phishing effort is relatively low in terms of cost and risk for the phishers. Further, phishers may reside in international locations that place them out of reach of authorities in the victim's jurisdiction, making prosecution much more difficult [33]. Phishers are rarely apprehended and prosecuted for the fraud they commit.

Developing methods for detecting phishing before any damage is inflicted is a priority, and several approaches for detection have resulted from the effort. Technical countermeasures, such as e-mail filtering and antiphishing toolbars, successfully detect phishing attempts in about 35 percent of cases [84]. Updating fraud definitions, flagging bogus Web sites, and preventing false alarms from occurring continues to challenge individual users and IT departments alike. An automated comparison of the design, layout, and style characteristics between authentic and fraudulent Web sites has been shown to be more promising than a simple visual inspection made by a visitor, but an up-to-date registry of valid and invalid Web sites must be available for such a method to be practical [55]. Because of ineffective technological methods of prevention, much of the responsibility for detecting phishing lies with the end user, and an effective strategy for guarding against phishing should include both technological and human detectors. However, prior research has shown that, like technology, people

are also limited in terms of detecting the fraud once they are coerced into visiting a bogus Web site [19]. Once the message recipient chooses to visit a fraudulent Web site, he or she is unlikely to detect the fraudulent nature of the request and the "hook" will have been set. In order to prevent users from sending sensitive information to phishers, educating and training e-mail users about fraud prevention and detection at the "bait" stage must be considered the first line of defense [53].

The goal of this paper is to better understand, given the large number of phishing attempts and the vast amount of attention given to phishing in the popular press, why users of online applications such as e-mail and instant messaging still fall prey to these fraudulent efforts.

Literature Review

RESEARCH INVESTIGATING DECEPTIVE COMMUNICATION has been conducted over the past several decades and has traditionally focused on the dyadic conversations between a deceiver and a receiver in a controlled laboratory setting. Much of the research has focused on the nonverbal deception indicators that are inadvertently transmitted by deceivers when telling lies [9, 18, 22]. A leading model with regard to computer-based interactions is the interpersonal deception theory (IDT) developed by Buller and Burgoon [7]. IDT proposes that deception occurs in a strategic fashion. Specifically, as the deceiver submits false information to its receivers in the midst of a conversation, then the deceiver seeks to observe signs of acceptance or disbelief. Then, depending on what signs are observed, the deceiver is able to either maintain the false account or make alterations in the hopes the account will become more acceptable. In other words, deceptive communication is modeled as an ongoing, interactive process.

Interpersonal Deception Theory and Phishing

In the case of phishing, however, the deceiver only has one opportunity to modify the false message, before the message is sent, because the communication takes place via e-mail. Also, the phisher cannot see the receiver's nonverbal behavior when reacting to the message and thus cannot monitor signs of disbelief and make strategic alterations to the message. The limited interaction between the phisher and receiver is illustrated using a truncated version of the original IDT model (see Figure 1). The differences between the two models may or may not hinder the deceiver's chances for success. The limited interaction with receivers can work to the deceiver's advantage, as the single deceptive phishing message cannot be directly compared by receivers to previous truthful messages for baseline comparison purposes. A corpus of messages can provide a holistic view of a deceiver's overall communication patterns, and deviations from the baseline messages can reliably point toward deception [87].

The shortened interaction illustrated by the truncated model of IDT can aid the phisher in other ways. Recent work by Park and colleagues [69] suggests that in traditional face-to-face communication, many people do not discover they have been lied to until well after the communication event has occurred. For someone who receives

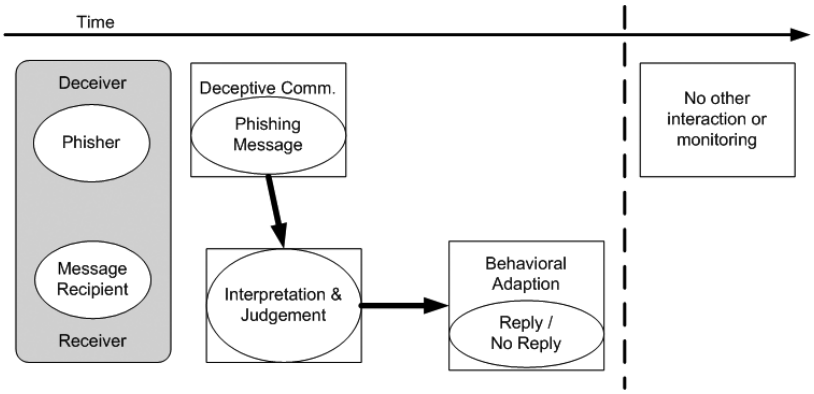


Figure 1. Truncated IDT Model for Phishing (adapted from [7])

a phishing message, the message receiver has ample time to uncover any discrepancies, largely due to the asynchronous nature of e-mail. Yet it seems that receivers make quick judgments on the veracity of a message, either by immediately deleting the message, by becoming suspicious and confirming suspicions with an external third-party source, or by being duped and responding with the desired information. Considering the importance of personal or financial information that is frequently solicited by phishers, a rapid response can be risky. Past research has suggested that after receivers "click" on the e-mail message, they rarely detect the phishing Web site or change their course of action [2, 19, 27, 46, 87]. Thus, the initial detection of the fraudulent e-mail is critical but can be difficult. Detecting the deceptive nature of a phishing e-mail is expected to depend on individual experiential and dispositional factors, which will now be discussed.

A Model for Deception in Phishing

Due to the inherent differences between users, this study focuses on examining what behavioral factors influence one's decision to respond to phishers. Figure 2 illustrates the relevant individual factors that are believed to have a direct effect on whether the receiver of a phishing e-mail will be deceived or not. This research model is based on Miller and Stiff's model [63] and the subsequent work of George and Carlson [10, 32]. These early models illustrate individual characteristics of the deceiver and receiver while also highlighting the potential the message has to directly influence the acceptance or rejection of said message. The characteristics of the communicators reflect typical individual and behavioral differences found within deceptive communication research. These include the motivation to deceive, the motivation to detect deception, the ability to encode a successful message, past experiences with deception, and other characteristics [10]. The communication medium is also modeled as having an influence, as its potential to convey the deceptive message should impact the outcome.

Aside from the deceiver's ability to communicate the message clearly while keeping unintended suspicious cues to a minimum [32], the medium being used to transmit

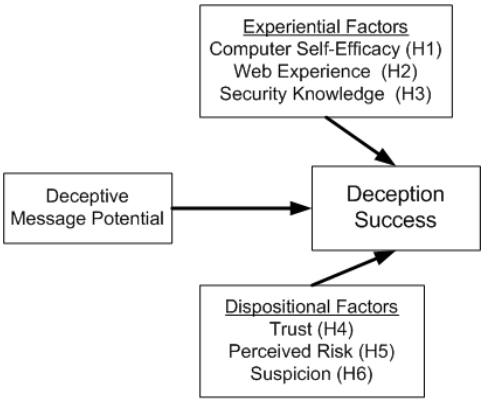


Figure 2. Research Model (adapted from [32])

the message influences the deceptive message potential for several reasons. First, the lower social richness and asynchronous nature of electronic media like e-mail can allow deceivers to rehearse and improve the message's deceptive potential [10, 17]. The *rehearsability* provided by a medium is only considered to be a factor during ongoing communication. This is because all media allow the initiator equal amounts of time to rehearse the message before the communicative process begins. Richer media such as face-to-face discussion, telephony, and videoconferencing provide faster feedback between conversants than media such as e-mail, preventing rehearsal from occurring during the conversation. Second, different media provide deceivers varying amounts of *tailorability,* described as the opportunity for the author to customize communication so that it becomes more acceptable to individual receivers [8, 12]. Finally, as mentioned in the previous discussion of IDT, different media transmit varied amounts of *social cues* that offer receivers a greater opportunity to develop suspicion and detect deception. A richer medium can transmit nonverbal visual and audio cues pointing to deception, such as gaze aversion or increased voice pitch, which less rich electronic media may restrict. Another way that phishing differs from face-to-face communication is that the initial phishing message is crafted for a mass audience rather than tailored for one individual receiver, and the message is planned and rehearsed to elicit a specific response with the requested information.

E-mail also provides a social cue advantage for phishers that more interactive scam artists do not have. Social engineering often tries to prey upon a target using elements of charm, sympathy, urgency, and similarity to make a message more believable. While it requires a savvy communicator to successfully convey those elements in rich, interactive communication without betraying deceptive intentions [64], phishers can craft a message using these same elements without having to risk leaking social indicators pointing to deception [72]. The research model presented here has been designed to reflect a less interactive environment than the previous models, with a "one-size-fits-all" deceptive message that is intended for a mass audience.

The earlier models incorporated the interactive, social context of the communication through the inclusion of interactive variables such as perceived social presence

and the level of personal experience with the other communicator [32]. In contrast to this, the current model includes two categories of individual factors and differences that are not contingent on interactive communication—namely, a category of three experiential factors (computer self-efficacy, Web experience, and knowledge of appropriate security policies) and a category of three dispositional factors (disposition to trust, perceived risk, and suspicion of humanity). Because the goal of the current research is to explore factors that can lead to the successful deception of a phishing receiver, the outcome variable of interest is labeled *deception success.* Therefore, the research question is centered on factors that contribute to deception success:

> *RQ: How do the experiential and dispositional characteristics of online users affect their susceptibility to potentially malicious phishing e-mails?*

Theoretical Analysis

IN THIS SECTION, SIX HYPOTHESES THAT PERTAIN TO THE NEW RESEARCH MODEL are developed. The first three hypotheses specify the expected relationships between the variables related to the receiver's experience with technology and the likelihood of deception success. Hypotheses 4, 5, and 6 are grouped as an individual's disposition to deception.

Experiential Factors

Computer self-efficacy (CSE) has been linked with online privacy concerns, in that Internet users with high CSE tend to be confident in their abilities to handle online threats and secure their privacy [85]. In regard to the threat of phishing, it is argued here that self-efficacy plays a significant role in susceptibility to Internet deception [2, 3, 19, 46]. Where the high CSE user is confident in his or her ability to deal appropriately with a phishing message, a user with low CSE is likely an inviting target for phishing efforts as he or she is often uncertain of what is being asked and is unlikely or unwilling to ask for advice [1]. Phishers often use strategies that present a dire problem to message receivers, such as lost customer records, problems accessing the customer's account for maintenance, or data integrity complications. This is typically followed by instructions to help assist receivers remedy the problem (i.e., by submitting personal information and passwords on the "hook" Web site). This is a common tactic used in social engineering that both introduces the problem and provides a solution in the same message [64]. Because of this, message receivers with low CSE, who are typically accustomed to receiving assistance from others, are likely to eagerly accept the provided solution without question [64]:

> *Hypothesis 1: Higher perceptions of CSE decrease the likelihood a person will be deceived by a phishing e-mail.*

Another possible experiential is one's experience with the communicative network used in the phishing attack, or the user's *Web experience.* According to channel expansion theory [11], communicators are affected by certain contextual factors

that can alter their perceptions of a particular communication medium. This theory proposes that the more experience a person involved in a conversation has, the better he or she will notice and process subtleties within the message, which provides for a richer communication event. Channel expansion theory proposes that noteworthy user experiences include the amount of experience a communicator has with his or her communication partners, the topic being discussed, the context surrounding the discussion and each communicator's relationship with it, and perhaps most relevant to a phishing event, the communication medium itself. Not only should experienced e-mail or instant message users be able to detect subtle cues pointing to deception that would otherwise attenuate in electronic media or pass without notice to inexperienced users [10], but experienced users tend to be more confident in their abilities to detect deceitful messages [16].

Furthermore, greater experience with the Web should also aid receivers when judging the veracity of a phishing e-mail message. Experienced users have past experiences with legitimate Web sites and e-mail exchanges for baseline comparison purposes. Jarvenpaa and Todd [47] found that the more Web experience consumers have, the more aware they are about potential risks and uncertainty surrounding potential transactions. Therefore, not only are experienced Web users better equipped to deal with deceptive cues within a message, they are also more likely to be aware of the threat of phishing, whereas inexperienced users may not be:

> *Hypothesis 2: Web experience decreases the likelihood that a person will be deceived by a phishing e-mail.*

The final experiential factor that should affect the success of phishing deception is the level to which the communicator is cognizant of different security threats, including phishing efforts, or *security awareness.* Security awareness training, as described by Straub and Welke [80], involves instructing Web users in the appropriate use of network and system resources. Not only should existing security policies be reviewed, but a description of possible threats and consequences of noncompliance should also be included. As mentioned earlier, users of online services are considered to be better prepared if they are made aware of the tactics involved in phishing and how to protect themselves from becoming victims or security risks [53]. Within organizations, a number of security lapses, such as naively giving out passwords and employee information, seem to correspond to the limited awareness of proper security measures [78]. Prior research has identified a number of security awareness initiatives, including network orientation and training, providing security procedure manuals, and issuing electronic newsletters, that have been tied into more effective security compliance and less user vulnerability [77, 79]. In terms of phishing, training communicators to find and identify any questionable motives when people report problems or make unexpected requests has shown to be effective for detecting deception [81].

Recent work on information privacy concerns in online environments gives further insight about the importance of security awareness when preventing threats such as phishing. Malhotra and colleagues [56] found that Web users who are concerned with information privacy and make information privacy a high priority report less trust and

perceive more risk when requested to share personal information, ultimately affecting their decisions to share information or not. Also, surveys indicate that most consumers hesitate before submitting personal information to companies if the receiver is unclear how the information will be used [43]. This hesitation suggests that these reticent Web users are aware of the potential consequences of sharing information and behave in a security-conscious fashion. Making Web users aware of similar questionable motives within e-mail communication should be beneficial for reducing user victimization from phishing:

> *Hypothesis 3: Security awareness decreases the likelihood a person will be deceived by a phishing e-mail.*

Dispositional Factors

The remaining three hypotheses examine the predicted relationships between the variables related to a receiver's disposition to deception and the likelihood of deception success. First, a person's disposition to trust is expected to be an important factor toward the phishing outcome. *Disposition to trust* refers to one's consistent willingness to believe and depend on others across many different contexts and situations [58]. People who report a high disposition to trust tend to have a high faith in humanity in general, which can manifest itself in electronic communication and online transactions with unfamiliar parties [59, 61]. Successful deception requires a certain amount of trust from the receiver or else the fabricated account behind the request for information will not be believed. With the unexpected request that is part and parcel to phishing, a propensity to trust is important for deception success as it reduces uncertainty between relational partners [40]. In an online environment, trust can take many different forms, whether it is a willingness to depend on others to deliver on promises and commitments, a belief that others will use one's personal information in an ethical manner, or a perception that any communication or transaction with another party will be kept secure [59]. Without a requisite level of trust, communicative exchanges and financial transactions are unlikely [30].

People differ in their disposition to trust others, and the more willing one is to trust others, the more likely one is to place trust in others before knowing background information about the trustee [57]. A person with high disposition to trust would be more apt to accept information from an online source at face value, even from unknown parties. In typical interpersonal communication, trust is usually built after a certain number of exchanges that exhibit trustworthy behavior have taken place [62], but in the case of phishing, there is no progression of e-mail exchanges between the phisher and the receiver to establish initial trust. Instead, phishers often embed familiar company names, logos, and slogans in the e-mail "bait" as a way to instill trust in the target, and they often resort to producing a mirror image of the legitimate site [29]. The familiar branding is used in order to produce, in the single message, the same level of trust that requires multiple messages in traditional communication to

build. We expect this is most likely to be achieved when the receiver of the phishing message has a high disposition to trust.

This tactic of mirroring legitimate sites does have a tendency to backfire on legitimate companies, particularly when their legitimate messages are received by people with low disposition to trust. Over time, some financial institutions have reported difficulties in communicating with customers using e-mail because many customers no longer trust legitimate messages coming from companies that they do business with [35]. These receivers seem unlikely to fall for phishing efforts and, if anything, are likely to make more false positive judgments of deception [4]. Therefore, we believe that a high disposition to trust serves to increase the chances of being deceived by phishing:

> *Hypothesis 4: Disposition to trust increases the likelihood a person will be deceived by a phishing e-mail.*

The research model also incorporates the likelihood that a person will partake in a risky behavior when interacting with unknown people, products, or services [25]. *Perceived risk* has been described as a dispositional factor that helps predict an individual's likelihood to accept risk in an uncertain situation [75]. All other things being equal, a person's "risk preference" is based on this trait and can be linked to his or her tendency to either be attracted or repelled by a risky choice [82]. A person's propensity to accept risk has been observed to be highly persistent, changing with time due to an accumulation of experiences [76]. Different people often perceive risk differently even when faced with the same situation and given the same choices by which to respond, and individuals with a disposition of high perceived risk will be more likely to proceed with behaviors of risk aversion. Prior research has illustrated how perceived risk can influence individuals in an online environment. For instance, Jarvenpaa and colleagues [48] speculate that people with high perceived risk would closely scrutinize Web sites before entering into a transaction and possibly require explicit information from a trusted source to remove any doubts, whereas people with lower perceived risk are less likely to hesitate before engaging in the transaction.

Within the context of phishing, individuals with high degrees of perceived risk should be concerned not only with the potential of being intentionally defrauded by another party but also by elements that can extend beyond either party's control, such as technical problems during an exchange or an unknown third party gaining access to the exchange through hacking. Thus, phishers often attempt to convey the notion of a secure environment by guaranteeing encrypted communication or by using temporary "throwaway" authenticated e-mail accounts as the source of the phishing message [2]. Likewise, impression formation makes a difference for people with higher perceived risk when deciding to pursue an exchange with a theretofore unknown party, and their judgments can be based on aspects ranging from information quality and appearance to misspelled words, grammatical errors, and download delays [23, 67]. As such, phishers certainly place high importance on impression management with regard to the "hooking" Web sites used to cull information, as the appearance is often appropriated directly from the legitimate, mimicked corporate Web site [55]. However, the initial

e-mail message is often lacking in quality [3], and risk-averse receivers may decide not to respond to such poorly crafted phishing requests:

> *Hypothesis 5: Higher perceived risk decreases the likelihood a person will be deceived by a phishing e-mail.*

One final dispositional factor that is expected to either result in deception success or in detection is the amount of suspicion a receiver attributes toward a phishing message. It is the receiver's *suspicion of humanity* that likely affects one's susceptibility to deception. Suspicion of humanity, which is the general assumption that other people are not well meaning [60], is a separate and distinct construct from disposition to trust; where a disposition to trust leads people to believe others by default, suspicion is instead considered a part of distrust and is more emotionally charged than a mere low level of trust [58]. A person with high suspicion of humanity takes a self-protective, defensive stance in situations in which their suspicion is aroused, and while a person with low disposition to trust also has a low sense of security, it is without the emotional response that accompanies suspicion of humanity. These responses often include worry, fear, and at their most extreme, paranoia. As Lewicki and colleagues put it, "trust expectations anticipate beneficial conduct from others, distrust expectations anticipate injurious conduct" [54, p. 444]. As such, a suspicion of humanity allows one to take a guarded approach in situations that do not offer security, with the added potential of the individual responding in a defensive manner. The potential trustee is likely to be avoided or treated in such a way as to minimize vulnerability [30].

Suspicion of humanity is activated when individuals perceive a lack of structural assurance in a given situation [61]. Put in the context of phishing, a person with a high disposition to trust will likely believe the other party by default, but a person carrying a high suspicion of humanity does not perceive an adequate level of protection from the other party and consequently perceives intentions of ill will. Familiar brands, logos, and trademarks are used by companies to provide such structural assurance. Therefore, one of a phisher's chief goals is to craft a realistic, professional-looking request that fails to arouse the receiver's suspicion. Without an appropriate amount of general suspicion to be aroused, we believe receivers with low suspicion of humanity are more likely to fall victim to phishing efforts:

> *Hypothesis 6: Suspicion of humanity decreases the likelihood a person will be deceived by a phishing e-mail.*

Research Methods

THE ABOVE SIX HYPOTHESES WERE TESTED using a field study in which each participant received a phishing e-mail asking for sensitive personal information. In practice, subjects can possibly receive several phishing e-mails a week. In this study, we specifically targeted information that we knew the subjects had. The study differed from traditional phishing schemes as the e-mails are usually not targeted for specific recipients. For example, a receiver might receive a phishing e-mail from someone pretending to be

Bank of America and asking for the receiver's password. This e-mail would be easily dismissed if he or she did not have an account at Bank of America.

Participants

The target population for this study was undergraduate business students enrolled in an introductory to information systems (IS) class at a large northwestern U.S. university. This course was a sophomore-level course that was required for all business majors; therefore, the course featured a broad cross section of all business majors. Most students were either sophomore (48 percent) or junior level (43 percent). The sample consisted of approximately 446 undergraduate students. The participants received course credit for their participation, which amounted to approximately 1 percent of their final grade. The average age of the subjects was 21.02, and the final sample included 189 male and 110 female subjects. On average, subjects reportedly spend 3.5 hours per week using computers, and none of the subjects indicated that they had previously been a victim of phishing.

A pilot study was conducted with 30 subjects in an introductory IS class four months prior to execution of the complete study. Based on this pilot, changes were made to the procedures and survey instrument. Changes to the instrument were based on a principal component analysis [68]. The pilot data were not included in the main data analysis. The main study ran nine weeks in its entirety. The first eight weeks consisted of Phase 1: Code and Policy Dissemination and Phase 2: SSC Usage and Security Training, and the last phase, Phase 3: The Phishing Attack, was executed in the ninth week.

Phase 1: Code and Policy Dissemination

The study began with the explanation to students that they could voluntarily participate in "security research." All students in the course volunteered and were issued an individual code, which was referred to as the "super-secure code" (SSC). The code was sealed in an official university envelope that included the university logo and contact information for the IT department. There was also a signature across the seal of the envelope. On the outside of the envelope was printed the subject's name and student number. The SSC was printed on official university letterhead with the title disclaimer "Do Not Disclose This Code."

The SSC itself was an easy-to-remember combination of letters and numbers (e.g., 76paris). The subjects were directed to use this code in conjunction with their student number to access a course management system that provided students access to current grading information, the ability to contact the professor or teaching assistants, and the ability to take online exams and quizzes throughout the semester. The students were told not to share the SSC with anyone under any circumstance as it would breach the secure grading process and could affect their grade for the class. Also, the students signed a nondisclosure agreement (NDA) in which they agreed to not disclose the SSC. The NDA included explicit language that informed students that disclosing the SSC to anyone would result in a violation of the university's student conduct code.

Following the issuance of the SSCs and NDAs, a brief survey was administered to the subjects. The survey included items that measured the disposition to trust [58, 59, 62], risk beliefs [48, 56], suspicion of humanity [58, 59], CSE [15], and Web experience [23], along with basic demographic information (see Appendix A).

Phase 2: SSC Usage and Security Training

Phase 2 consisted of the eight weeks following the survey administration. During this time, a unit on Internet security and privacy was taught among the regular class material. Within this unit, the instructor taught the concepts of phishing, hacking, and other relevant security/privacy topics. After completion of the security concepts, the subjects were given a 15-question multiple-choice assessment to objectively capture their awareness of IS security concepts. These questions were generated from a test bank associated with a prominent introductory management information systems (MIS) textbook [49]. Each subject's proficiency on the assessment was used to measure security awareness in the research model. Throughout Phase 2, every student used the SSC an average of five to six times a week to access lecture notes, take exams, and complete other class-related activities. These activities served to reinforce the students' belief that the SSC was important and should be kept private. At the beginning of every class meeting, a PowerPoint slide was displayed reminding students not to disclose their SSC.

It must be noted that during week six of Phase 2, all the participants, along with everyone else at the university, were subjected to an actual (and unplanned) phishing attack. In this case, the phishing e-mail told members of the university credit union that their password had been compromised and the receivers needed to click on a link to change their password. Following this phishing attempt, the technology management department e-mailed a warning to all students advising them not to respond to the request and to report any such scams. Further, there was an article in the student newspaper detailing the phishing attack.

Phase 3: The Phishing Attack

After week eight, students were asked via e-mail to disclose the SSC in a phishing-type scenario by the researchers. Specifically, each student was presented a situation in which there was a dire need to forward his or her SSC to a database administrator. In keeping with typical phishing messages [3], grammatical errors were included in the e-mail. The message, sent from a "database administrator" named "Jason Roth," was as follows:

> This e-mail is to inform you of a problem we are having with the information technology database. Due to a data collision we have lost some information and are unable to recover it. In order to get the database back up and working we need you to forward us your "super-secure code." Please respond to this e-mail with your code. Sorry for the inconvenience.

Based on experiences learned from the pilot study, collection of the SSC was allowed to continue for seven days after the phishing message was sent. The pilot study revealed that a two-week period could be problematic, as the IT group in campus and the class instructor were increasingly contacted by more and more students asking for guidance about the phishing attacks after the first week concluded, and the number of responses to the message decreased sharply after a week.

Deception success was coded as "1" when the subject answered the deception e-mail with the correct SSC (97 out of 299 subjects = 32 percent). Deception success was deemed to have occurred in instances in which the student answered the e-mail with the correct SSC. A failure was coded as "0" when the receiver either (1) failed to respond to the e-mail (170/299 = 57 percent), (2) alerted someone else about the phishing e-mail (26/299 = 9 percent), (3) responded with a question or comment to the phishing e-mail (4/299 = 1 percent), or (4) responded with incorrect information to the phishing e-mail (2/299 < 1 percent).

After seven days the research team debriefed the subjects as to the actual purpose of the study. Prior to the debriefing, we administered the postinstrument, which measured subjects' beliefs about the importance of the SSC. These items, used for manipulation checks, are displayed in Table 1. The details of study were then revealed and subjects were asked to forward the original phishing e-mail to the researchers. This was to verify that they had seen the e-mail and were able to make a judgment about the phishing message. Students who could not find or did not receive the e-mail were dropped from the subsequent data analysis. In all, 92 percent of the students did respond that they had received an e-mail from "Jason Roth."

Data Analysis

THE MESSAGE WAS SENT TO 446 SUBJECTS, but 147 subjects were excluded from the subject pool for one of four reasons: (1) those who dropped the class (11 subjects), (2) those who did not receive the e-mail or could not find the e-mail when asked in the follow-up survey (101 subjects),[1] (3) those who did not complete all the items for the two surveys (27 subjects), and (4) those who did not complete or take the objective security assessment during phase two of the study (8 subjects). This left the final subject pool at 299.

Although the percentage of people who responded with their SSC was high (97/299 = 32 percent), as mentioned before, this phishing exercise had the benefit of targeting information that the researchers knew the subjects had. Also, this study did not take into account technology barriers that might have prevented messages from being acted on or viewed. Information regarding which e-mail service was used by the subject was also captured in order to test if some services provided better security against phishing attacks. Consistent with past research, not a single subject noted that their e-mail provider detected the message as possible phishing [84]. Also, we found that no one provider did a better job in filtering our e-mail messages, and there was no significant loss of subjects from any particular e-mail service.

Table 1. Manipulation Check Descriptive Statistics

	Mean for nondeceived	Standard deviation	Mean for deceived	Standard deviation	*p*-value	Standard deviation
How risky did you perceive responding to the e-mail with your super-secure code?	4.23	1.79	4.36	1.57	0.53	1.72
By answering the phishing e-mail, would class policy be violated?	5.15	1.68	4.74	1.50	0.95	1.64
If you did respond to the (phishing) message with your super-secure code, did you believe you would be punished?	4.86	1.68	4.56	1.66	0.88	1.68
Cronbach's alpha	0.804					
Grand mean	4.75		4.55		0.80	

Manipulation Check

One concern resulting from the methodology used was whether or not the emphasis placed on the SSC was viewed as valid by the subjects. The research team wanted to verify that the subjects believed that by revealing their code to anyone else, they would be in violation of class policy and the student conduct code. As part of the second survey, given prior to the debriefing, three questions concerning the importance of securing the SSC were given. Had there been a difference in the perceived validity between the subjects who answered the e-mails with their SSC and those who did not answer the e-mail, the results could have been confounded and the analysis of any further data would possibly have been trivial. However, the results of the manipulation check suggest that the subjects did feel that the SSC and the NDA were important and enforceable. It is important to note that there was no difference in the perceived importance of the SSC between those who were deceived and those who did not respond ($F = 1.363$, $p = 0.09$ for a one-tailed t-test). The means for the three items were all above average, which suggests that the SSC was taken seriously by the subjects overall.

Results

MPLUS VERSION 5.1 WAS USED FOR DATA ANALYSIS. Mplus was chosen over other structural equation modeling (SEM) packages such as Amos, PLS-Graph, or LISREL due to its ability to estimate paths using categorical variables as outcomes. SEM analysis was chosen over regression analysis as it can be used to test all paths on the research model simultaneously [31]. The estimation methods for binary endogenous variables can be calculated by using either maximum likelihood (ML), weighted least squares (WLS), or weighted least squares and variance adjustment (WLSMV) [66]. Simulation research has shown that using WLSMV is preferable to WLS and ML in cases in which a binary endogenous variable is modeled [65]. Where WLS uses the full weight matrix, WLSMV uses the diagonal of the weight matrix in the estimation, which allows the residuals to be closer to zero than other estimation techniques, and therefore the estimates seem to be more consistent.

Following advice from Brown [6] given for SEM analysis, the results from a power analysis were used to guide model respecification. The complete instrument, before respecification, included the following measures: CSE (ten items), Web experience (four items), disposition to trust (three items), suspicion of humanity (six items), and risk perceptions (five items). In this study, comparative fit statistics for evaluating the model included the comparative fit index (CFI), which should be above 0.90, and the Tucker–Lewis index, which should be less than the CFI but still above 0.90 [6]. Badness of fit was assessed using the weighted root mean square residual (WRMR), which should be less than 0.90 [65], and root mean square error of approximation (RMSEA), which is recommended to be less than 0.08 [6].

A descriptive analysis was undertaken in SPSS 12.0 to evaluate the distribution of the sample. A statistical power analysis was also conducted in order to ensure

an appropriate sample size was available for testing the omnibus structural model. Because the current study features a binary outcome as the dependent variable, the Monte Carlo approach is appropriate for power analysis [6]. There were several assumptions and specifications that were met for the Monte Carlo approach to power analysis. These include normally distributed indicators without missing data, which was consistent with the data set, a sample size of at least 250, the number of replications of at least 10,000, and the population parameter estimates for indicators were 0.8 [66].[2] The Monte Carlo simulation conducted with Mplus provided evidence that the scales would cause power problems at sample sizes of 250, 300, 350, 400, 450, and 500. Specifically, the confidence intervals and the bias of the CSE and suspicion of humanity parameters did not fall within the required specifications. For this reason, the original ten-item CSE measure developed by Compeau and Higgins [14] was modified to a five-item measure, based on the pilot results and the face validity of the items. Similar, five-item measures of CSE have been used in prior research [44, 73]. As with CSE, the suspicion of humanity scale was truncated due to unacceptable standard errors in the power analysis. Again, this three-item measure was guided by the extant literature (e.g., three-item use in a prior study) [28]. A subsequent power analysis provided validation of the adjusted scales for CSE and suspicion of humanity. All of the above criteria provided by Muthen and Muthen [66] were met in this subsequent Monte Carlo power analysis.

The next step in the analysis was to provide a measurement model to assess both convergent and discriminant validities. To evaluate convergent validity, a factor analysis was undertaken (see Appendix B). As stated above, there were 19 vetted items administered to the subjects. The factor analysis was conducted using the principal components method and constrained the number of factors extracted to five, as per the above research model. Promax rotation with Kaiser normalization was used in the extraction process.[3]

Further confirmatory factor tests were executed to assess the measurement model more rigorously. When assessing the appropriateness of the measurement model, one should examine (1) the reliability of items, (2) the composite reliability of the constructs, and (3) the average variance extracted (AVE) by the constructs. This examination of reliability was done for the latent variables within the research model. Because the dependent variable was measured dichotomously, it was not included in this analysis. Due to the fact that the objective measure of security awareness was an index score, this was excluded from the AVE analysis, as index scores are not appropriate for convergent and discriminant validity testing [68]. In this instance, face validity and reliability were tested. This operationalization of Internet security knowledge is consistent with past research that used other objective measures. For example, past literature has used objective measures in the context of SEM analysis in similar fashion such as vividness [42], effort [39], and user performance [83]. This objective measure was specifically chosen to measure Internet security rather than using past subjective instrumentation [20].

Reliability analysis is a basis to evaluate the internal consistency of a measurement instrument. The most common statistic for evaluating reliability is Cronbach's alpha.

In this research, the instrument is validated relative to a theoretical perspective, it is recommended that reliabilities result in 0.70 or higher [68]. The instrument tested provided high reliability to the latent factors as measured (Table 2). The results show that each item shows convergence to its proper latent factor. Composite reliability was analyzed next on the bank of items to provide further reliability analysis. As shown, all reliabilities were greater than the recommended threshold of 0.70 [41].

Convergent validation provides an understanding of which observed variable correlates with which latent factors. Mplus was used to assess the convergent validity of the items. In this case, validity was evaluated using the AVE for each construct. These values should be greater than 0.5 [26], and as they were, the constructs were judged to have convergent validity. To establish discriminant validity, the same AVE values for each construct should be larger than its correlations with the other constructs, which Table 3 demonstrates. All individual items loaded onto the appropriate factor, and none of items loaded above 0.5 onto any other factor. Finally, none of the constructs correlate higher than the suggested limit of 0.85 [51]. Overall, the constructs used in the measurement model displayed sufficient convergent and discriminant validity.

Having established the measurement model to be valid, we then evaluated the structural model using Mplus. Based on five common fit statistics, the evaluated model showed sufficient goodness of fit. The SEM analysis (reported in Figure 3) revealed that higher CSE ($\beta = -0.348$, $p < 0.05$), increased Web experience ($\beta = -0.361$, $p < 0.05$), increased security knowledge ($\beta = -0.413$, $p < 0.05$), and a higher suspicion of humanity ($\beta = -0.150$, $p < 0.05$) all had significant negative effects on deception success, supporting Hypotheses 1, 2, 3, and 6. The paths that were not significant were disposition to trust ($\beta = -0.050$, $p > 0.05$) and risk beliefs ($\beta = 0.004$, $p > 0.05$). In this study, the independent variables account for 36.4 percent of the variance (R^2) in deception success.

To summarize, four of the six hypothesized factors had a significant influence on the likelihood that Web users will be successfully deceived by a phishing e-mail. As Hypothesis 1 stated, subjects who reported a higher CSE and are likely to be more self-reliant when faced with new problems online are found to be less likely to cede control of their information assets to an unknown party, no matter how official the request may appear. Likewise, subjects reporting higher degrees of Web experience appear to be better equipped to process unexpected requests for information and, in the case of phishing, decide not to respond to the requests altogether, as Hypothesis 2 outlined. Finally, subjects who showed high proficiency on security awareness evaluations seem to utilize earlier advice and training and refused to honor the request for information, supporting Hypothesis 3.

Discussion

ALL IN ALL, EXPERIENCE AND TRAINING appear to be the most effective tools for guarding against phishing. Earlier studies have reached similar conclusions with other types of deception and have called for awareness programs to sensitize Web users to the undesirable dangers that they are exposed to online [36, 37]. The results here show

Table 2. Measurement Model: Composite Reliabilities

Item	Loadings	Composite reliabilities	Cronbach's α
CSE1	0.84	0.92	0.90
CSE2	0.87		
CSE3	0.78		
CSE4	0.82		
CSE5	0.88		
WebExp1	0.79	0.84	0.82
WebExp2	0.76		
WebExp3	0.71		
WebExp4	0.78		
ISK	N/A	N/A	N/A
Trust1	0.81	0.86	0.86
Trust2	0.80		
Trust3	0.87		
Risk1	0.78	0.90	0.90
Risk2	0.82		
Risk3	0.89		
Risk4	0.87		
Susp1	0.85	0.85	0.92
Susp2	0.78		
Susp3	0.80		

Notes: Scale: seven-point Likert, 1 = "strongly disagree" to 7 = "strongly agree." CSE = computer self-efficacy, WebExp = Web experience, Susp = suspicion of humanity, ISK = Internet security knowledge, N/A = not available.

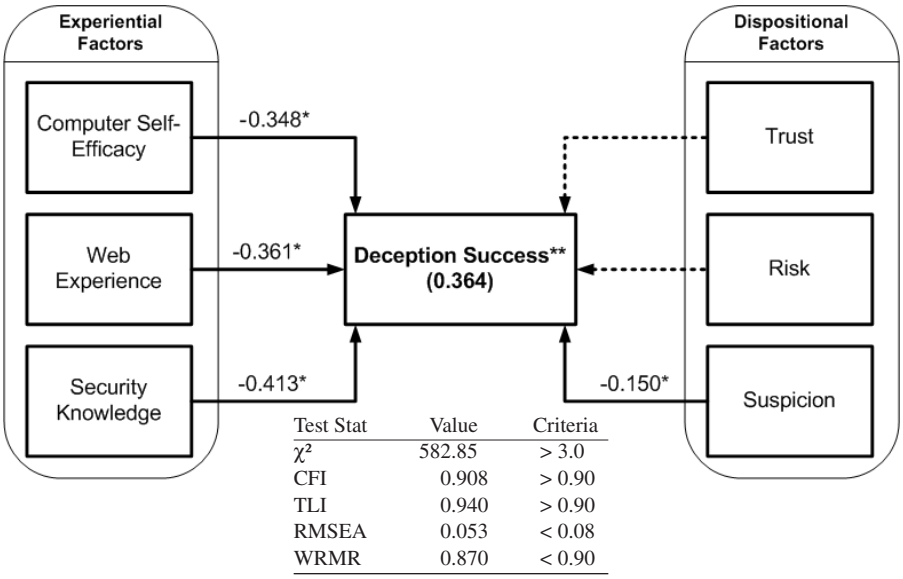
Table 3. Factor Intercorrelations

	CSE	WebExp	Trust	Risk	Susp	ISK
CSE	**0.704**					
WebExp	0.375	**0.573**				
Trust	0.034	0.006	**0.863**			
Risk	0.006	–0.010	0.199	**0.704**		
Susp	0.002	–0.010	0.030	0.004	**0.657**	
ISK	0.140	0.210	0.020	0.151	0.006	**N/A**

Notes: AVE values are shown in boldface on the diagonal. CSE = computer self-efficacy, WebExp = Web experience, Susp = suspicion of humanity, ISK = Internet security knowledge, N/A = not available.

that subjects rating low on experiential factors are most prone to deception, which affirms the strategy of phishers and other social engineers: it is more productive to prey on the vulnerable and the naive for personal information.

Of the three hypothesized dispositional factors (disposition to trust, perceived risk, and suspicion), however, only Hypothesis 6, which predicted a relationship between



Test Stat	Value	Criteria
χ^2	582.85	> 3.0
CFI	0.908	> 0.90
TLI	0.940	> 0.90
RMSEA	0.053	< 0.08
WRMR	0.870	< 0.90

Figure 3. Results of the Structural Analysis

suspicion of humanity and deception success, was supported. Given the amount of classroom exposure subjects had to topics related to Internet security, it seems unlikely that those who still did not look upon the message with suspicion would respond to the request in anything other than a compliant fashion. The hypotheses for disposition to trust and risk beliefs, however, were not supported. Overall, the subject pool reported to be well above average in terms of disposition to trust (a mean of 5.04 on a seven-point scale) and also reported to be closer to average with regard to risk beliefs (4.46). This result runs counter to past research on deceptive communication and phishing, as both disposition to trust and perceived risk factors have helped explain why people release personal information to unknown entities online [56].

In the current study, though, these two beliefs did not discriminate between those who did release their SSC and those who did not. One possible explanation is derived from the work of Miller and Stiff [63], who surmised that some people fear the consequences of a wrong judgment where deception is concerned and, because of possible interpersonal and economic repercussions, become less motivated to detect lies. In this study, it is possible that the risk of not responding with the SSC and facing a disruption to student access to class resources could have outweighed the security risks of defying the class policy. In other words, the need to access lab and testing software on a daily basis was critical for success in the class, and the potential lack of accessibility could have been viewed as having more immediate repercussions than the possible consequences of illicitly submitting the SSC.

Although the current study is quantitative in nature, it must be noted that the return e-mails from those who were deceived provided some insights into the process that subjects underwent in answering the e-mails. Most subjects who did respond to the phishing message responded like this student did:

> Here is my SSC XXXXXX. I hope that the database will get fixed very soon. Best of luck to you on fixing the database.

We also found some subjects gave away more than just the requested information:

> My Network ID is XXXXX, My Student Number is XXXXX, my super secure Code is XXXXX, my home number is XXXXX.

> I think this is my code: XXXX, but I'm not sure. You can call my mom at XXX-XXXX if this isn't it as she will have it for you.

Other e-mail responses from subjects who were not deceived reiterated the strength of the manipulation and illustrated the security awareness of some subjects, demonstrating the desired influence of sound training and security policies on user mindfulness and subsequent behavior:

> I was told to never give out my super secrete (sic) code. . . . So how do I know this isn't a scam?

> I'm sorry to hear about your problems, but I will not be able to assist you.

Limitations and Implications

Before discussing the potential contributions of this research, its limitations must be addressed and should be considered when evaluating the findings described above. First, the subjects in this study were undergraduate students, which often casts aspersions on the generalizability of results. In addition, subjects were all enrolled at the same university, which introduces the possibility that the subjects could have been influenced by an idiosyncratic phenomenon. Students are likely inappropriate for studies that involve outcome variables [45], but they are suitable for studies that involve process variables [38, 50], such as deception detection. Further, the students who participated in this study reflect the general population in that they all had active e-mail accounts, making them as susceptible to phishing as anyone. A second limitation involved the actual phishing attack that occurred during the study, which may have had an impact on the results by potentially heightening the awareness of the subjects. It is possible that the relationships to suspicion and the security knowledge could have been increased. However, a recent finding from Downs and colleagues suggests that, although some people are aware of phishing e-mail, they do not link this awareness to their own vulnerability or to strategies for identifying phishing attacks [21]. This was likely the case in the current study, though none of the 26 subjects who successfully detected the phishing attempt in the research study mentioned the real phishing attack during later interviews. A third limitation related to the study design involved the measurement of risk perceptions. The items for the risk perception measure were not modified to fit the general context. As the scale was administered before the phishing event, the items were instead crafted for accepting risk of providing "personal or sensitive information to online companies" in order to not inadvertently reveal the purpose of the study.

This research included strict coding of the phishing response. This was a choice made by the research team, as it was difficult to rationalize coding anyone as being deceived who did not explicitly give the requested sensitive information. In the end, it would be impossible to know for certain the subject's intent. By coding the outcome variable strictly, there would be no question as to the legitimacy and correctness of the outcome variable, although the research team does concede this might also lead to a different kind of bias.[4]

The next limitation deals with the phishing effort used in this study, which consisted of a sole e-mail message without an accompanying Web site. In other words, the procedures in this study only involved the "bait" portion of the "bait-and-hook" strategy used commonly by phishers. The "bait" appeared to have been produced by someone connected to the same organization as the message receivers, which would be difficult for many phishers to produce. As mentioned before, prior research suggests that Web users are not likely to detect the false nature of the mocked Web sites used in phishing; however, the results here indicate that the e-mail message alone was sufficient to successfully deceive a significant number of subjects. It is believed that this limitation, as well as other circumstances, makes the findings about users' susceptibility to phishing stronger. First, not only was the "bait" alone effective for retrieving sensitive information, the message was completely fabricated. Further, instead of mentioning a serious event such as the "data collision" in class, course instructors continually repeated the need to keep the SSC private. Finally, our phishing effort also came on the heels of the aforementioned phishing attack on campus, which could have also impeded deception success. Given all these circumstances, a low success rate would have been reasonable, yet a third of the receivers complied with the request. Nevertheless, future research can help determine if there are different influences involved and whether a different number of subjects, larger or smaller, would have responded to a request accompanied by a fake Web site.

A final limitation of the study is the asynchronous nature of the communicative medium, e-mail, and how it inhibits the ability to measure response time from the receiver. The amount of time between the receiver downloading and responding to the phishing message might indicate the amount of scrutiny given to the message, and it seems likely that the subjects who were deceived in this study responded quickly, without hesitation. Despite being able to send the messages to all the subjects simultaneously, however, there is no way of determining exactly when receivers first accessed the message, so response time is difficult to ascertain.

Contributions to Research

WHILE DECEPTION IN FACE-TO-FACE COMMUNICATION is still being investigated by researchers, the increased popularity of computer-mediated communication (CMC) requires researchers to consider how deception can be transmitted electronically, perhaps more easily than more traditional modalities. This, in turn, requires researchers to reexamine earlier theory on deceptive communication in order to apply it to CMC. The current study takes a step in this direction. First, the long-established interpersonal deception

theory was drawn upon, but adapted for a more asynchronous, CMC event. In doing so, the new, truncated model illustrates the less personal, less immediate CMC modality, focusing entirely on the initial message, without the strategic modifications to subsequent messages the deceiver makes according to IDT. By only using the "bait" portion of a "bait-and-hook" phishing attempt, the study provides evidence that deception online does not need to be strategic in order to be effective. As unusual and implausible as it was, the initial message from the fictitious "Jason Roth" was ample communication for eliciting private information from the subjects. Beyond establishing a familiar social categorization ("the university database administrator") for the receiver's appraisal, the phisher simply has no interest in establishing relational familiarity or engaging in prolonged communication with the receiver. Any subsequent message from the phisher (including the strategic modifications modeled by IDT) only improves the chances that the phisher will contradict him- or herself or arouse suspicion in the receiver. Unfortunately, "Jason" was able to elicit the desired information by merely appearing to be part of the receiver's social category. The same tactic could easily be attempted on e-mail users within organizations in which individuals are unlikely to have relational familiarity with every other organizational member.

It is believed that the same limited amount of strategy exhibited in phishing can also be seen in other online scams, such as in online auction scams and in developing Web sites for the purpose of propagating malware. Like phishing messages, they are crafted for wide audiences of no particular target, they are impersonal, and they are active for only days at a time. The truncated model presented in this study could help shed light on research that investigates these criminal activities, as well as investigations into other forms of online communication. For instance, it may also help explain the dissatisfactory results of legitimate online activities, such as how a lack of prolonged communication between buyers and suppliers in online reverse auctions can lead to misunderstandings, strained relationships, and ultimately, distrust [13].

Likewise, the individual variables posited by the CMC-adapted model by Carlson and George [10] were tested as being motivation for receivers to detect deception. To the knowledge of the research team, no previous study has examined the specific experiential and dispositional variables that were focused on here, but given the amount of variance explained by the research model, future work in this area should account for them in addition to other situational and media-based variables. For instance, deception researchers have noted the differences in synchronicity between face-to-face communication and computer-mediated modalities such as e-mail and instant messaging and how turnaround time can affect the content of responses [86]. Rather than take advantage of response latencies to rehearse responses or, more important, closely scrutinize messages from others, many people tend to respond quickly and reciprocate the other party's communication patterns. In phishing, response latencies are especially critical because there is only one message that can be evaluated. Users placing high in the experiential factors and on suspicion of humanity could be among those who use response latencies to their benefit, provided they have the experience to delay responding quickly and the suspicion necessary to closely examine the request.

Implications for Practice

For managers, the results presented here should provide welcome news: experiential factors appear to be more influential to a user's susceptibility to phishing and online deception than dispositional factors. Dispositional factors, such as those measured in this study, naturally vary between individuals and are more stable over time than the experiential factors, such as CSE, Web experience, and security awareness, which tend to improve with time within users. Thus, a well-planned security program, which is discussed below, should provide the means for managers to target these experiential factors and reinforce sound security policies that are consistent for all users.

According to Straub and Welke [80], a rigid security program includes actions that are devoted to deterrence and act to reduce the perpetrator's chances for success and reduce the target's likelihood of being victimized (see also [35]). Currently, there are two main methods for deterring phishing. The first is through automated means, such as through antiphishing software and toolbars that are now available widely from Internet service providers. Unfortunately, automated means are often ignored or misunderstood by users [84]. The key to success with antiphishing software lies with the ability of the user to make the right decision based on information given to the user by the software [21, 74]. As noted by Sheng et al., "there is always a case with this software where people have to make decisions on their own" [74, p. 89].

The second popular method for deterring phishing involves educating users [24], a method that the current results suggest holds the most potential. Institutions such as the New York State government have adopted contextual training in which users are sent simulated e-mail phishing and are given materials at the end of the study on combating phishing [34]. Another approach to training is called the embedded approach, wherein users role-play on a mocked-up e-mail inbox and are presented with several different scenarios. Participants are exposed to several types of e-mail phishing and are able to experience the results of appropriate and inappropriate responses [52, 74]. Such tools not only provide experiential education but aim to improve Web users' self-efficacy as well, as they gain confidence dealing appropriately with strange requests made via e-mail. Although initial results of these methods are promising, it is unclear if users develop an understanding of how the training tools differ from their own mail client. The results of the current research suggest that improving the CSE could contextualize the issues that occur throughout a normal working day so that informed decisions can be made correctly about incoming e-mails. Likewise, the gain in Web experience and increased security knowledge resulting from training should make users less susceptible to deception. Table 4 summarizes how our findings integrate with the contemporary antiphishing tools and training methods.

Overall, "quick fix" solutions probably will not provide long-term deterrence, as attack methodologies do change, and simple zero-tolerance policies may not produce desirable results. An easy rule of thumb for managers and employees might simply be to refuse to honor an unexpected request for information from a stranger, but such a policy could produce "false positive" judgments and prevent valid requests from being fulfilled. Rather, the current, truncated model of IDT suggests that e-mail users

Table 4. A Summary of Deficiencies in Contemporary Antiphishing Methods

	Description	CSE	WebExp	ISK	Susp	Notes
Software	Informs users of possible problems and allows them to make decisions based on more information.			♦	•	Although software does raise suspicion, they are somewhat of a black box to users. It still comes down to people making a decision on whom to trust.
Contextual training	Sending simulated phishing messages to users, then following up with education material.			•	•	This type of training will raise awareness, but again the user still lacks an understanding of how the security systems work, if at all.
Embedded training	Simulating a work environment and providing scenario training on particular e-mails.	♦	♦	•	•	Promising but still needs to integrate basic computer training and Internet training to cover all the factors.

Notes: • = significant coverage, ♦ = some coverage, blank cell = no coverage. CSE = computer self-efficacy, WebExp = Web experience, ISK = Internet security knowledge, Susp = suspicion of humanity.

should actively engage and prolong the conversation with people making requests for information through e-mail, in the hopes of either validating legitimate requests or deterring the phishers who have no desire to extend the communication.

The results presented here indicate, as Grazioli and Jarvenpaa [37] and other information security advocates have found, that the most effective way to combat deception online is to educate Web users on the tactics used by social engineers such as phishers. Technological tools, such as phishing toolbars and e-mail filters, can be effective as long as security definitions are kept current, but even then the risk of "false positive" judgments can result in errors in caution. The Web user is the last line of defense, and given the current state of technology, potentially the most accurate judge. Instituting policies that require workers to maintain active communication with someone requesting information could be effective in combating phishers, especially if combined with two- or three-factor authentication ("who you are, what you have, and what you know") or "speak-easy" security (a shared secret between communicators). Such policies could help eliminate the noninteractive phishers as well as identify messages from seemingly familiar sources that have been spoofed.

Notes

1. A decision was made by the research team to only include subjects who could provide evidence they received the phishing e-mail. An analysis of variance (ANOVA) was conducted to see if these subjects possessed any difference in individual behavioral traits from that of the subjects in the final pool. No statistical differences were found for all six constructs ($p > 0.05$ for all six constructs).

2. Muthen and Muthen [66] posit the following criteria for determining sample size: (1) bias of the parameter and the associated standard errors do not exceed 10 percent for any parameter, (2) any factor covariance standard error does not exceed 5 percent, and (3) the coverage at the 95 percent confidence is between 0.91 and 0.98.

3. The goodness-of-fit test proved significant ($p < 0.001$), and both the Kaiser–Meyer–Olkin (KMO) and the Barlett's test provided values of 0.943 and $p < 0.001$. The pattern matrix clarified the reduction process, further providing that all items loaded above 0.6 and with no cross-loadings above 0.3.

4. The model was reanalyzed to include one subject who responded with a question to the phishers or responded with incorrect information. This model did not statistically increase the overall fit of the model to the data.

References

1. Ahuja, M.K., and Thatcher, J.B. Moving beyond intentions and toward the theory of trying: Effects of work environment and gender on post-adoption information technology use. *MIS Quarterly, 29,* 3 (2005), 427–459.

2. Bellovin, S.M. Spamming, phishing, authentication, and privacy. *Communications of the ACM, 47,* 12 (2004), 144.

3. Berghel, H. Phishing mongers and posers. *Communications of the ACM, 49,* 4 (2006), 21–25.

4. Biros, D.; George, J.; and Zmud, R. Inducing sensitivity to deception in order to improve decision making performance: A field study. *MIS Quarterly, 26,* 2 (2002), 119–144.

5. Bond, C.F., and DePaulo, B.M. Accuracy of deception judgments. *Personality and Social Psychology Review, 10,* 3 (2006), 214–234.

6. Brown, T.A. *Confirmatory Factory Analysis for Applied Research.* New York: Guilford Press, 2006.

7. Buller, D., and Burgoon, J.K. Interpersonal deception theory. *Communication Theory, 6,* 3 (1996), 203–242.

8. Burgoon, J.; Bonito, J.; and Kam, K. Communication and trust under face-to-face and mediated conditions: Implications for leading from a distance. In S. Weisband and L. Atwater (eds.), *Leadership at a Distance.* Mahwah, NJ: Lawrence Erlbaum, 2004.

9. Burgoon, J.; Buller, D.; Ebesu, A.; and Rockwell, P. Interpersonal deception: V. Accuracy in deception detection. *Communication Monographs, 61,* 4 (1994), 303–325.

10. Carlson, J.R., and George, J. Media appropriateness in the conduct and discovery of deceptive communication: The relative influence of richness and synchronicity. *Group Decision and Negotiation, 13,* 2 (2004), 191–210.

11. Carlson, J.R., and Zmud, R. Channel expansion theory and the experiential nature of media richness perceptions. *Academy of Management Review, 42,* 2 (1999), 153–170.

12. Carlson, J.R.; George, J.F.; Burgoon, J.K.; Adkins, M.; and White, C.H. Deception in computer-mediated communication. *Group Decision and Negotiation, 13,* 1 (2004), 5–28.

13. Charki, M., and Josserand, E. Online reverse auctions and the dynamics of trust. *Journal of Management Information Systems, 24,* 4 (Spring 2008), 175–197.

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

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

16. Cooper, R., and Kahai, S. Exploring the core concepts of media richness theory: The impact of cue multiplicity and feedback immediacy on decision quality. *Journal of Management Information Systems, 20,* 1 (Summer 2003), 263–299.

17. Dennis, A.R.; Fuller, R.M.; and Valacich, J.S. Media, tasks, and communication processes: A theory of media synchronicity. *MIS Quarterly, 32,* 3 (2008), 575–600.

18. DePaulo, B.; Lindsay, J.J.; Malone, B.E.; Muhlenbruck, L.; Charlton, K.; and Cooper, H. Cues to deception. *Psychological Bulletin, 129,* 1 (2003), 74–118.

19. Dhamija, R.; Tygar, J.D.; and Hearst, M. Why phishing works. In R. Grinter, T. Rodden, P. Aoki, E. Cutrell, R. Jeffries, and G. Olson (eds.), *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* New York: ACM Press, 2006, pp. 581–590.

20. Dinev, T., and Hart, P. Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce, 10,* 2 (Winter 2005–6), 7–29.

21. Downs, J.; Holbrook, M.; and Cranor, L. Decision strategies and susceptibility to phishing. In L.F. Cranor (ed.), *Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS).* New York: ACM Press, 2006.

22. Ekman, P.; O'Sullivan, M.; Friesen, W.; and Scherer, K. Face, voice, and body in detecting deceit. *Journal of Nonverbal Behavior, 15,* 2 (1991), 125–135.

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

24. Evers, J. Security expert: User education is pointless. *CNET News,* 2009 (available at http://news.cnet.com/2100-7350_3-6125213.html).

25. Featherman, M.S., and Pavlou, P.A. Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human–Computer Studies, 59,* 4 (2003), 451–474.

26. Fornell, C., and Larcker, D.F. Evaluating structural equations models with unobservable variables and measurement error. *Journal of Marketing Research, 18,* 1 (1981), 39–50.

27. Fu, A.Y.; Wenyin, L.; and Deng, X.T. Detecting phishing Web pages with visual similarity assessment based on earth mover's distance (EMD). *IEEE Transactions on Dependable and Secure Computing, 3,* 4 (2006), 301–311.

28. Gabrieal, I.J., and Nyshadham, E. A cognitive map of people's online risk perceptions and attitudes: An empirical study. In R.H. Sprague (ed.), *Proceedings of the 41st Annual Hawaii International Conference on System Sciences.* Los Alamitos, CA: IEEE Computer Society Press, 2008 (available at www.computer.org/portal/web/csdl/doi/10.1109/HICSS.2008.6).

29. Gartner survey shows phishing attacks escalated in 2007; More than $3 billion lost to these attacks. Press Release Gartner, Stamford, CT, December 17, 2007 (available at www.gartner.com/it/page.jsp?id=565125).

30. Gefen, D.; Benbasat, I.; and Pavlou, P. A research agenda for trust in online environments. *Journal of Management Information Systems, 24,* 4 (Spring 2008), 275–286.

31. Gefen, D.; Straub, D.; and Boudreau, M. Structural equation modeling and regression: Guidelines for research practice. *Communications of the AIS, 4,* 7 (2000), 1–77.

32. George, J.F., and Carlson, J.R. Group support systems and deceptive communications. In R.H. Sprague (ed.), *Proceedings of the 32nd Annual Hawaii International Conference on System Sciences.* Los Alamitos, CA: IEEE Computer Society Press, 1999, pp. 1–10.

33. Goldsmith, J., and Wu, T. *Who Controls the Internet? Illusions of a Borderless World.* New York: Oxford University Press, 2006.

34. Gone phishing . . . A brief on anti-phishing exercise. New York State Office of Cyber Security & Critical Infrastructure Coordination, New York, 2005.

35. Goth, G. Phishing attacks rising, but dollar losses down. *IEEE Security & Privacy, 3,* 1 (2005), 8.

36. Grazioli, S., and Jarvenpaa, S. Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. *IEEE Transactions on System, Man, and Cybernetics, 30,* 4 (2000), 395–410.

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

38. Greenberg, J. The college sophomore as guinea pig: Setting the record straight. *Academy of Management Review, 12,* 1 (1987), 157–159.

39. Gretzel, U., and Fesenmaier, D.R. Persuasion in recommender systems. *International Journal of Electronic Commerce, 11,* 2 (Winter 2006–7), 81–100.

40. Gulati, R., and Gargiulo, M. Where do interorganizational networks come from? *American Journal of Sociology, 104,* 1 (1999), 1439–1493.

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

42. Hess, T.; Fuller, M.; and Mathew, J. Involvement and decision-making performance with a decision aid: The influence of social multimedia, gender, and playfulness. *Journal of Management Information Systems, 22,* 3 (Winter 2005–6), 15–54.

43. Hoffman, D., Novak, T., and Peralta, M. Building consumer trust online. *Communications of the ACM, 42,* 4 (1999), 80–85.

44. Hsieh, J.J.P.-A.; Rai, A.; and Keil, M. Understanding digital inequality: Comparing continued use behavioral models of the socio-economically advantaged and disadvantaged. *MIS Quarterly, 32,* 1 (2008), 97–126.

45. Hughes, C., and Gibson, M.L. Students as surrogates for managers in a decision-making environment: An experimental study. *Journal of Management Information Systems, 8,* 2 (Fall 1991), 153–166.

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

47. Jarvenpaa, S.L., and Todd, P. Consumer reactions to electronic shopping on the World Wide Web. *International Journal of Electronic Commerce, 2,* 1 (Fall 1997), 59–88.

48. Jarvenpaa, S.L.; Tractinsky, N.; and Saarinen, L. Consumer trust in an Internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication, 5,* 2 (2000), 45–71.

49. Jessup, L., and Valacich, J. *Information Systems Today.* Upper Saddle River, NJ: Pearson Prentice Hall, 2005.

50. Kacmar, M.; Ratcliff, S.; and Ferris, G. Employment interview research: Internal and external validity. In R.W. Eeder and G.R. Ferris (eds.), *The Employment Interview: Theory, Research, and Practice.* Newbury Park, CA: Sage, 1989, 32–42.

51. Kline, T. *Psychological Testing: A Practical Approach to Design and Evaluation.* London: Sage, 2005.

52. Kumaraguru, P.; Rhee, Y.; Acquisti, A.; Cranor, L.; Hong, J.; and Nunge, E. Protecting people from phishing: The design and evaluation of an embedded training email systems. In

B. Begole, S. Payne, E. Churchill, R. St. Amant, D. Gilmore, and M.B. Rosson (eds.), *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* New York: ACM Press, 2007.

53. Larcom, G., and Elbirt, A.J. Gone phishing. *IEEE Technology and Society Magazine, 25,* 3 (2006), 52–55.

54. Lewicki, R.; McAllister, D.; and Bies, R. Trust and distrust: New relationships and realities. *Academy of Management Review, 23,* 3 (1998), 438–458.

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

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

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

58. McKnight, D.H., and Chervany, N. What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *International Journal of Electronic Commerce, 6,* 2 (Winter 2001–2), 35–59.

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

60. McKnight, D.H.; Kacmar, C.; and Choudhury, V. Dispositional trust and distrust distinctions in predicting high- and low-risk Internet expert advice site perceptions. *e-Service Journal, 3,* 2 (2004), 35–58.

61. McKnight, D.H.; Kacmar, C.; and Choudhury, V. Whoops . . . Did I use the wrong construct to predict e-commerce trust? Modeling the risk-related effects of trust versus distrust concepts. In R.H. Sprague (ed.), *Proceedings of the 36th Annual Hawaii International Conference on System Sciences.* Los Alamitos, CA: IEEE Computer Society Press, 2003 (available at www.hicss.hawaii.edu/HICSS36/HICSSpapers/INCRM04.pdf).

62. McKnight, H.; Cummings, L.L.; and Chervany, N. Initial trust formation in new organizational relationships. *Academy of Management Review, 23,* 3 (1998), 473–490.

63. Miller, G.R., and Stiff, J.B. *Deceptive Communication.* London: Sage, 1993.

64. Mitnick, K.D., and Simon, W. *The Art of Intrusion.* Indianapolis: Wiley, 2005.

65. Muthen, B. Goodness of fit with categorical and other non-normal variables. In K.A. Bollen and J.S. Long (eds.), *Testing Structural Equation Models.* Newbury Park, CA: Sage, 1993, 205–243.

66. Muthen, L.K., and Muthen, B. *Mplus User's Guide.* Los Angeles: Muthen & Muthen, 2007.

67. Nicholson, D.; Nicholson, J.; Parboteeah, V.; and Valacich, J. Using distraction-conflict theory to measure the effects of distractions on individual task performance in a wireless mobile environment. In R.H. Sprague (ed.), *Proceedings of the 38th Annual Hawaii International Conference on System Sciences.* Los Alamitos, CA: IEEE Computer Society Press, 2005 (available at www.computer.org/portal/web/csdl/doi/10.1109/HICSS.2005.657).

68. Nunnally, J.C., and Bernstein, I.H. *Psychometric Theory.* New York: McGraw-Hill, 1994.

69. Park, H.S.; Levine, T.; McCornack, S.; Morrison, K.; and Ferrara, M. How people really detect lies. *Communication Monographs, 69,* 2 (2002), 144–157.

70. Phishing activity trends report. Anti-Phishing Working Group. Chicago, 2006.

71. Protecting against phishing by implementing strong two-factor authentication. White Paper, RSA Security, Bedford, MA, 2008.

72. Rao, S., and Lim, J. The impact of involuntary cues on media effects. In R.H. Sprague (ed.), *Proceedings of the 33rd Annual Hawaii International Conference of System Sciences.* Los Alamitos, CA: IEEE Computer Society Press, 2000.

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

74. Sheng, S.; Magnien, B.; Kumaraguru, P.; Acquisti, A.; Cranor, L.F.; Hong, J.; and Nunge, E. Anti-phishing Phil: The design and evaluation of a game that teaches people not to

fall for phish. In L.F. Cranor (ed.), *Proceedings of the Third Symposium on Usable Privacy and Security (SOUPS).* New York: ACM Press, 2007.

75. Sitkin, S., and Pablo, A. Reconceptualizing the determinants of risk behavior. *Academy of Management Review, 17,* 1 (1992), 9–38.

76. Sitkin, S., and Weingart, L. Determinants of risky decision-making behavior: A test of the mediating role of risk perceptions and propensity. *Academy of Management Journal, 38,* 6 (1995), 1573–1592.

77. Spurling, P. Promoting security awareness and commitment. *Information Management & Computer Security, 3,* 2 (1995), 20–26.

78. Stanton, J.M.; Stam, K.R.; Mastrangelo, P.; and Jolton, J. Analysis of end user security behaviors. *Computers & Security, 24,* 2 (2005), 124–133.

79. Straub, D.W. Effective IS security: An empirical study. *Information Systems Research, 1,* 2 (1990), 255–277.

80. Straub, D.W., and Welke, R.J. Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22,* 4 (1998), 441–469.

81. Vrij, A. *Detecting Lies and Deceit: The Psychology of Lying and the Implications for Professional Practice.* Chichester, UK: John Wiley & Sons, 2000.

82. Weber, E., and Milliman, R. Perceived risk attitudes: Relating risk perception to risky choice. *Management Science, 43,* 2 (1997), 123–145.

83. Webster, J., and Ahuja, J.S. Enhancing the design of web navigation systems: The influence of user disorientation on engagement and performance. *MIS Quarterly, 30,* 3 (2006), 661–678.

84. Wu, M.; Miller, R.C.; and Garfinkel, S.L. Do security toolbars actually prevent phishing attacks? In R. Grinter, T. Rodden, P. Aoki, E. Cutrell, R. Jeffries, and G. Olson (eds.), *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* New York: ACM Press, 2006.

85. Yao, M.Z.; Rice, R.E.; and Wallis, K. Predicting user concerns about online privacy. *Journal of the American Society for Information Science & Technology, 58,* 5 (2007), 710–722.

86. Zhou, L. An empirical investigation of deception behavior in instant messaging. *IEEE Transactions on Professional Communication, 48,* 2 (2005), 147–160.

87. Zhou, L.; Burgoon, J.K.; Twitchell, D.P.; Qin, T.; and Nunamaker, J.R., Jr. A comparison of classification methods for predicting deception in computer-mediated communication. *Journal of Management Information Systems, 20,* 4 (Spring 2004), 139–166.

Appendix A. Survey Instrument

Variable/ item code	Item	Item adapted from
Computer efficacy[1]		[15]
Complete the following sentences: "I could complete most jobs using an unfamiliar software package . . .		
CSE1	If I could call someone for help if I got stuck.	
CSE2	If someone else had helped me get started.	
CSE3	If I had a lot of time to complete the job for which the software was provided.	
CSE4	If I had just the built-in help for assistance.	
CSE5	If someone showed me how to do it first.	
Web experience[2]		[23]
On average, how much time per week do you spend on each of the following Web activities?		
WebExp1	Reading news on the Web?	
WebExp2	Reading and/or posting messages to social sites?	
WebExp3	Accessing information on the Web about products and services you may buy?	
WebExp4	Shopping (e.g., actually purchasing something) on the Web?	
Disposition to trust[3]		[58]
Trust1	I usually trust people until they give me a reason not to trust them.	
Trust2	I generally give people the benefit of the doubt when I first meet them.	
Trust3	My typical approach is to trust new acquaintances until they prove I should not trust them.	
Risk beliefs[3]		[48, 56]
Risk1	In general, it would be risky to give (my information) to online companies.	
Risk2	There would be high potential for loss associated with giving (my information) to online firms.	
Risk3	There would be too much uncertainty associated with giving (my information) to online firms.	
Risk4	Providing online firms with (my information) would involve many unexpected problems.	
Suspicion of humanity[3]		[61]
Susp1	People are usually out for their own good.	
Susp2	People pretend to care more about one another than they really do.	
Susp3	Most people inwardly dislike putting themselves out to help other people.	

Notes: [1] Seven-point Likert scale, 1 = "not confident at all" to 7 = "totally confident." [2] Seven-point scale, none/1–30 minutes/30–60 minutes/1–2 hours/2–4 hours/4–8 hours/8+ hours. [3] Seven-point Likert scale, 1 = "strongly disagree" to 7 = "strongly agree."

Appendix B. Factor Analysis

Components	1	2	3	4	5	Mean	Standard deviation
CSE5	**0.95**	0.02	–0.12	0.04	0.03	5.8	1.04
CSE2	**0.83**	0.02	0.01	–0.02	–0.09	3.9	1.54
CSE4	**0.82**	0.09	–0.00	0.04	–0.06	5.3	1.44
CSE1	**0.74**	–0.07	0.02	0.03	0.14	4.3	1.59
CSE3	**0.63**	–0.06	0.24	–0.13	0.01	4.9	1.18
Risk3	0.00	**0.95**	–0.01	–0.03	–0.09	4.5	1.30
Risk4	–0.03	**0.88**	0.03	0.02	0.06	4.3	1.24
Risk2	0.03	**0.87**	0.03	–0.03	–0.02	4.7	1.20
Risk1	0.01	**0.81**	–0.03	0.03	0.12	4.8	1.33
WebExp4	–0.03	–0.02	**0.87**	–0.05	0.02	5.6	1.46
WebExp1	–0.02	0.11	**0.86**	0.02	–0.07	5.3	1.24
WebExp2	0.02	–0.07	**0.78**	0.03	0.08	5.7	1.18
WebExp3	0.04	0.01	**0.78**	0.05	–0.03	6.2	1.00
Trust3	–0.00	–0.01	0.02	**0.90**	–0.01	4.9	1.40
Trust1	0.01	0.06	–0.06	**0•.89**	–0.07	5.1	1.42
Trust2	0.00	–0.07	0.07	**0.87**	0.06	5.1	1.25
Susp1	0.04	–0.02	–0.03	0.01	**0.88**	4.2	1.24
Susp3	–0.03	0.06	–0.04	0.02	**0.86**	4.5	1.20
Susp2	–0.01	0.01	0.06	–0.04	**0.86**	4.5	1.19
ISK (index score)						75.7	15.99

Notes: CSE = computer self-efficacy, WebExp = Web experience, Susp = suspicion of humanity, ISK = Internet security knowledge. Extraction method: principal component analysis. Rotation method: promax with Kaiser normalization; rotation converged in six iterations. Boldface numbers indicate the factor on which each item most appropriately loaded.