MESSAGE QUALITY AND QUANTITY MANIPULATIONS AND THEIR EFFECTS ON PERCEIVED RISK

(Authors Names Withheld for Anonymity)

ABSTRACT

As we are continually confronted with increasingly sophisticated electronic messages, determining valid from deceptive messages has become an extremely important task. The present study leverages the lens of information manipulation theory to analyze the impact of perceived message quality and quantity on perceived source competence and message honesty, and their subsequent impact on perceived risk. We administered phishing scenarios to respondents and evaluated their responses to survey items related to the given scenario. The data support that perceived message honesty, support, and technology anxiety influence risk perceptions of a message. In addition, the quality of a message strongly influences individual perceptions of honesty.

KEYWORDS: Information Manipulation Theory; source competence, risk; technology anxiety; truth bias; direct experience; support; phishing, scenario

INTRODUCTION

Distinguishing between valid and deceptive messages is critical for protecting information, especially given that anyone can publish information online and that there is an increasing concern for privacy and security. Although computer users may increasingly become aware of current privacy and security threats, cybercriminals may adapt to user responses by crafting increasingly creative deceptive messages. If malicious messages go undetected, potentially harmful communications could threaten the security of organizations and/or individuals.

Buller and Burgoon (1996) determined that a quarter of all person-to-person conversations contain deception or suspected deception. Park et al. (2002) found that, of all detected deception, 24.7% is detected in less than a day, 45.3% within a week, 65.9% within a month, and 83.4% within a year. Ideally, this evidence shows that important decisions should be made over longer spans of time; however, deception detection often requires immediate response (Park et al., 2002) and identifying deceptive cues may be difficult. In fact, cues of deception are different than they used to be. Earlier theories, such as Interpersonal Deception Theory (Buller & Burgoon, 1996), focused on cues in verbal and nonverbal person-to-person communication. However, visible cues – e.g., competence, composure, sociability, and dynamism – regarding the communicator's believability are absent in digital communication mediums such as email, instant messaging, text messaging, etc. In addition, rehearsability – the degree which media gives participants time both before and during an interaction to plan, edit, and rehearse the information in and presentation of their messages (George & Robb, 2008) – is more prevalent in digital communication and permits deceivers to craftily refine their message, making it more difficult to detect deception. Understanding that deception can pose substantial risk for companies and individuals, we seek to find explanations for the following research questions:

RQ1: How do message manipulations (e.g. quantity, quality, relation, and clarity maxims) affect the security perceptions for a given solution? Which manipulations increase/decrease the perceived risk in computer mediated messages?

RQ2: Does technology anxiety restrict one's perceptions of risk over computer mediated mediums?

RQ3: Does an individual's perceptions of risk of computer mediated communications increase with the help from a third party?

Traditionally, the Cooperative Principle (Grice, 1989) and Information Manipulation Theory (IMT; McCornack, 1992; McCornack, Levine, Solowczuk, Torres, & Campbell, 1992) evaluate the impacts on perceived message integrity from the amount of information in the message (quantity), the veracity of the message (quality), the relevance of the information (relation), and the clarity of the message (manner). For example, using scenario evaluation, McCornack et al. (1992) measured the variables of IMT using interpersonal face-to-face communication. They successfully argued that manipulations in quantity, quality, relation, and manner affect individual perceptions of honesty and perceptions of competence. For example, messages that include too much or too little information may violate the quantity maxim, fabricated messages may violate the quality maxim, messages that do not address the real issue or seem to be out of context may violate the relation maxim, and messages that lack of detail or clarity may violate the manner maxim. Each of these violations may cause receivers to have lower perceptions of message honesty and lower perceptions that the message source is competent. However, message manipulations in digital communication may be drastically different because of reduced non-verbal and paraverbal cues and increased rehearsability. These foundations inform our research efforts to determine how message manipulations in digital communication, specifically message quantity and quality manipulations, may affect perceptions of risk.

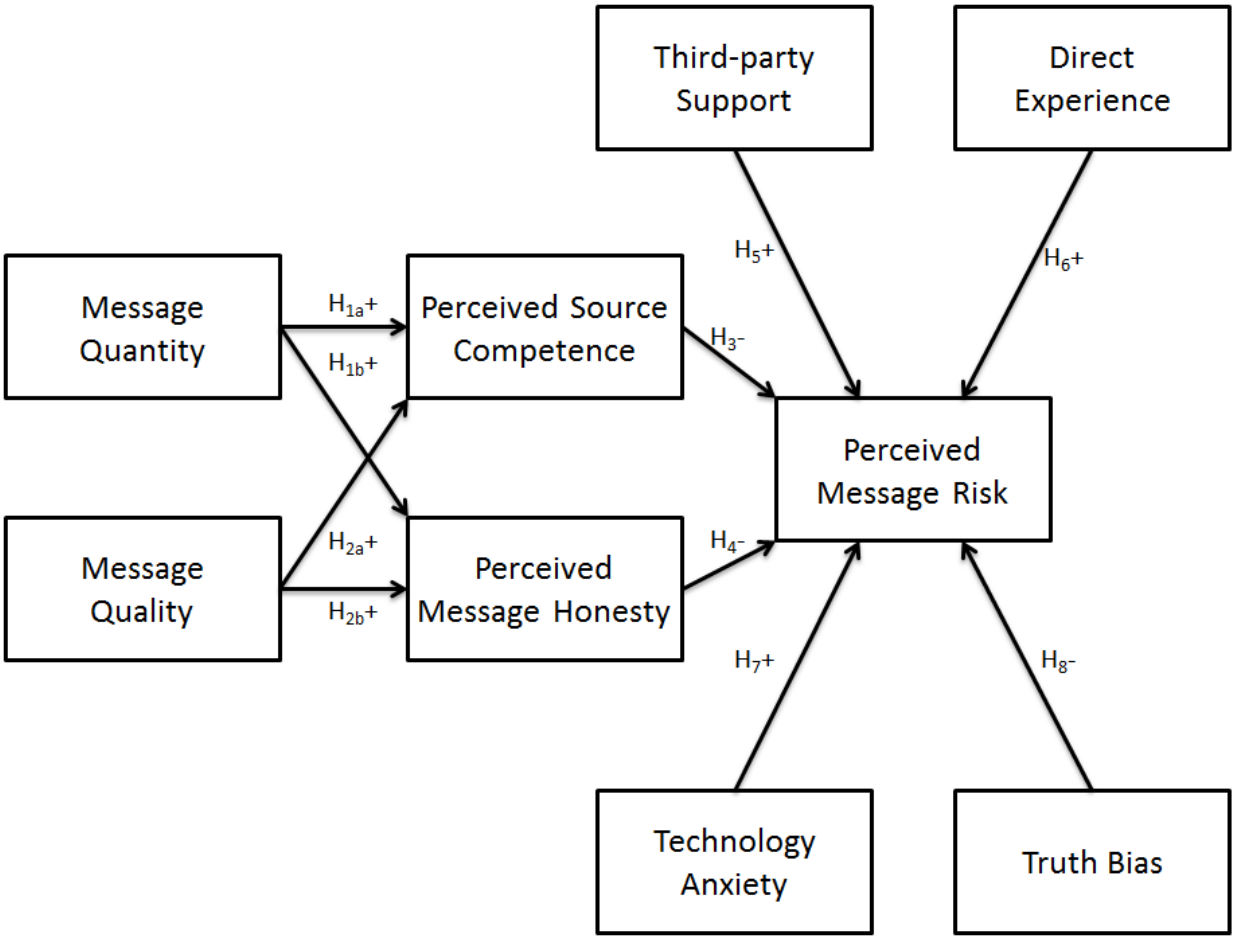
The remainder of our paper proceeds as follows: In the next section, we will discuss relevant literature, present our conceptual model, and postulate our hypotheses. In the following section, we will discuss our research design and methods for validating our model. Finally, we will present results and discuss implications.

THEORETICAL BACKGROUND

Computer and information systems are constantly under attack, making outside threats a great concern for companies. For example, the Hactivist group "Anonymous" recently sold the source code for PCAnywhere because Symantec failed to pay their ransom (Hachman, 2012). The way individual employees respond to attacks from outside the organization can result in information theft or loss. One way criminals attack is through the process of cognitive hacking, by targeting human perceptions and corresponding behaviors (Enrici, Ancilli, & Lioy, 2010). The two main types of cognitive hacking are pretexting – the use of scenarios to encourage people to provide information when they would not normally – and phishing (Anderson, 2008). Phishing attacks use emails, fake websites, or malicious software to direct users to fraudulent websites to steal personal information, credentials, and financial data (Enrici et al., 2010). Both types of attacks either seek to establish interpersonal relationship to garner trust and commitment or to manipulate perception, belief, and behavior to incite emotions of excitement or fear (Dolan,

2004). If an employee falls victim to cognitive hacking, outsiders may steal, damage, or destroy company or personal information. Helping individuals understand the potential existing threats and risks involved may help companies and individuals adequately protect their information. Through proper training of employees, individuals may acquire the tools necessary to perceive risks involved in responding to cognitive hacking. This paper suggests some of the factors which influence the perceived risk of messages and our conceptual model of these factors is illustrated in **Error! Reference source not found.**.

Figure 1: Conceptual Model



Perceived Message Risk

Considering the importance of perceived risk on behavior, perceived threat severity, and perceived threat susceptibility, we examine factors that affect perceived risk of messages. Perceived risk is defined as a person's subjective belief of suffering a loss in pursuit of a desired outcome (Pavlou, 2003), including the uncertainty and adverse consequences of using a product or service (Dowling & Staelin, 1994). Featherman and Pavlou (2003) examined the impact of perceived risk on the variables of the technology acceptance model (TAM) such as perceived usefulness, perceived ease of use, and adoption intention and found that perceived risk is a

barrier to consumer behavior. In fact, Pavlou (2003) determined that the reduction of perceived risk will increase a consumer's willingness to transact. In addition, perceived risk reduces perceptions of control (Jarvenpaa, Tractinsky, & Vitale, 2000). When considering behavior, perceived risk increases when circumstances arouse feelings of uncertainty, discomfort, concern, and/or anxiety (Dowling & Staelin, 1994). Furthermore, Dinev and Hart (2006) stated that a tolerance threshold exists at which users determine whether it is worth the risk to provide personal information online due to security, virus, and spoof threats. For example, users who believe a message's intent is to phish information will not act on the message, considering the risks involved. We believe the following factors explain individual perceptions of overall risk to some degree.

Message Quantity and Quality

Individuals process messages hundreds of times a day when reading information over the web, interacting with others in person, chatting with others online, etc. Successfully identifying which of these messages are accurate and complete may prove difficult. To better distinguish between these messages, we draw upon IMT (McCornack, 1992; McCornack et al., 1992), which discusses the ways messages are often manipulated to deceive the message recipient. Two key maxims of IMT pertain to manipulations in the quantity (amount) and the quality (accuracy) of information conveyed. An illustration of the violation of these two maxims is through a phishing message. (The other two maxims will be evaluated subsequently in another project.) With the prevalence of increasingly sophisticated phishing messages, the threat against individual and organizational information is real. However, any noticeable change in the message dimensions addressed by these two maxims could help users identify legitimate messages from their counterparts.

In information security, quantity manipulations may include missing company signatures, the lack of seals, the absence of contact information, or especially incomplete message content. Quality manipulations occur when messages distort sensitive information or completely fabricate information. For example, a phishing message may include misspellings, grammatical errors, unrecognized sender emails, and inappropriate calls to action. With these manipulations, individuals interpret the competency of the sender as well as the honesty of the message. From this we propose:

H1a: Message quantity is positively associated with perceived source competence.
H1b: Message quantity is positively associated with perceived message honesty.
H2a: Message quality is positively associated with perceived source competence.
H2b: Message quality is positively associated with perceived message honesty.

Perceived Source Competence

Source competence refers to the message recipient's perceptions about the knowledge or expertness of the source (Berlo & Lemert, 1961) and is linked to message acceptance (Berlo, Lemert, & Mertz, 1969; Pornpitakpan, 2004). Furthermore, messages which contain more information than specifically requested (McCornack, 1992) and messages which aren't fully disclosive reduce perceived source competence (McCornack et al., 1992). Based on the previous

literature, a successful phishing attack purporting to come from a competent source may be readily accepted despite the risks involved. Therefore, we predict:

H3: Perceived source competence is negatively associated with perceived message risk.

Perceived Message Honesty

When interpreting the honesty of messages, individuals rely on subtle cues in making judgments (McCornack et al., 1992). Although these cues may be perceived to be honest or dishonest, an individual's interpretation of them may be erroneous. If an individual perceives a message is honest, they are likely to act on the message, despite the inherent risks. In the case of a phishing message, incorrect judgments could affect company and individual information. We then hypothesize that:

H4: Perceived message honesty of the message is negatively associated with perceived message risk.

Third-party Support

Park et al. (2002) determined that individuals rely on third parties or physical evidence to facilitate lie detection when interpreting messages. Even though an individual may not intentionally harm a company by heeding false messages, their acts may dramatically reduce the protection of company resources. Sitren & Applegate (2007) state that individuals are less willing to commit crime when they have support from others. In the context of our study, we believe individuals will be less likely to commit acts that could potentially harm a company if they feel they can receive support. Through the help of management or peer support, employees can make better decisions and avoid possible threats. This support could not only aid in identifying misleading or false messages, but also train users to recognize these cues on their own.

An additional avenue of support to users for making an informed decision is through assurance mechanisms in the message itself. Grazioli and Jarvenpaa (2000) mention that assurance mechanisms could include seals to provide site authentication, warranties to ensure products are backed by the company, news clips to offer third party reviews or endorsements, and physical location to ensure situational normality. Situational normality is defined as a properly ordered setting to facilitate a successful transaction (McKnight, Cummings, & Chervany, 1998). These assurance mechanisms give individuals access to more information when judging a message, and the lack of these mechanisms may cause users to perceive a message as risky. Therefore, we propose:

H5: Third-party support is positively associated with perceived message risk.

Direct Experience

Direct experience is defined as prior interaction with or personal involvement with something (e.g. with a computer virus infection, identity theft, receipt of phishing e-mail) by the individual in question (Boss, Kirsch, Angermeier, & Boss, 2009). The experienced user is more inclined to

convert intentions into behavior (Ajzen & Fishbein, 1980; Taylor & Todd, 1995). Accordingly, individuals who have had more positive experiences with a specific medium of communication are more likely to continue using the medium and the opposite is true for individuals who have had negative experiences (King & Xia, 1997). Therefore, an individual exposed to negative experience with a phishing email may be more skeptical of other emails. Drawing from criminology literature, Boss et al. (2009) determined that direct experience had an effect on individual perceptions of risk. These risk perceptions result in defensive behaviors. Based on the previous literature, we predict that:

H6: Direct experience is positively associated with perceived message risk.

Technology Anxiety

Kinard, Capella, and Kinard (2009) determined that technology adoption is a function of attitude towards the technology and an individual's degree of technology anxiety. Individuals who experience technology anxiety fear that technology use could lead to the loss of important data or other possible mistakes (Thatcher & Perrewé, 2002). Technology anxiety is a precursor to self-efficacy (Marakas, Yi, & Johnson, 1998). In essence, individuals who experience less technology anxiety feel they can appropriately respond to situations dealing with technology. A person who is more anxious with technology may be more likely to perceive everything as risky or everything as valid which may have adverse effects because individuals may label valid messages as risky or risky messages as valid. This could lead to one of two undesired results: (1) individuals may accept risky messages because they fear neglecting a valid message or (2) individuals may reject valid messages because they fear following a risky message. Therefore, we posit that:

H7: Technology anxiety is positively associated with perceived message risk.

Truth Bias

Truth bias is a presumption of truthfulness or inherent belief that people are telling the truth (Boyle, 2003). Individuals with strong truth bias are more likely to judge others as truthful, ultimately reducing judgmental accuracy (Stiff, Kim, & Ramesh, 1992). Applying this to the security context, we propose that individuals who generally give others the benefit of the doubt are more likely to judge outside attacks such as phishing to be truthful. So in essence, these individuals overlook the risks involved and fall victim to such attacks exposing individual and company information. Therefore, we posit that:

H8: Truth bias is negatively associated with perceived message risk.

METHOD

Subjects

Subjects were drawn from undergraduate students of a large comprehensive university with 114 total usable responses. These students were offered a small credit to their overall grade as compensation for their participation. Participants of the study followed an email link to an online

survey in which they responded to items to determine their perceptions of a given scenario. The first screen pertains to informed consent, followed by exposure to exposure to the treatments and instrument as described below. Subject evaluations were compared across groups based on the scenarios that subjects were exposed to.

Design

To test our hypotheses, we conducted a 2 (Message Quantity: low, high) x 2 (Message Quality: low, high) scenario-based factorial design. Both Message Quantity and Message Quality were manipulated between subjects. Variations in message quantity and quality occurred by deleting or altering information. The process model illustrated in Figure 2 indicates the flow of our instrument. Prior to scenario exposure, we measured technology anxiety, truth bias, and third-party support. Then the participants were randomly assigned to one of four conditions: (1) low quality - low quantity, (2) high quality - low quantity, (3) low quality - high quantity, and (4) high quality - high quantity. Figure 3 and
Figure **4** are examples of two of these scenario conditions. Even though quantity manipulations are apparent in these conditions, quality manipulations are more subtle such as an additional "s" in the sender email account, http instead of an https link, grammar mistakes, misspellings, and improper capitalization. After the scenario, respondents were asked questions regarding their previous experience with similar messages, their perceptions of the quality and quantity of the message, their perceptions of the message honesty and competence of the message source, and their perceptions of the risk involved in acting on the message. The order of these items is critical so the measurement of one construct does not bias items of the following constructs. For example, improper order of early measures and conditions could prime participant responses towards later items.

Figure 2: Instrument Flow

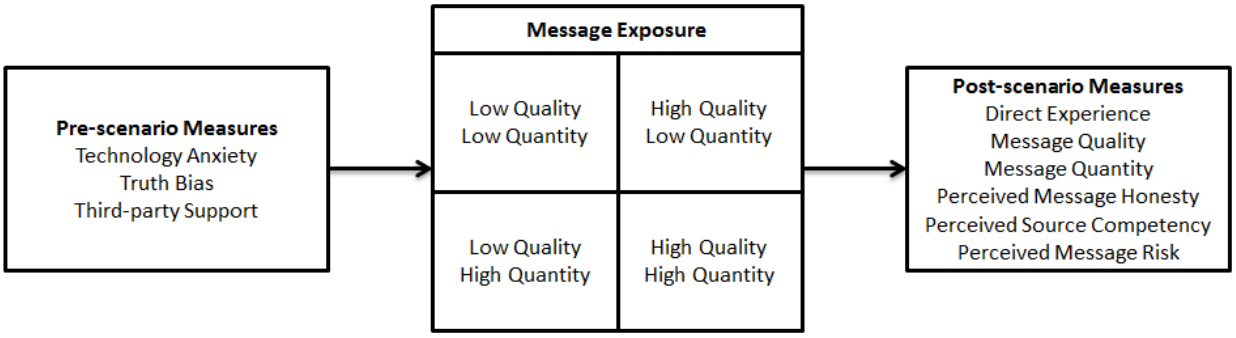
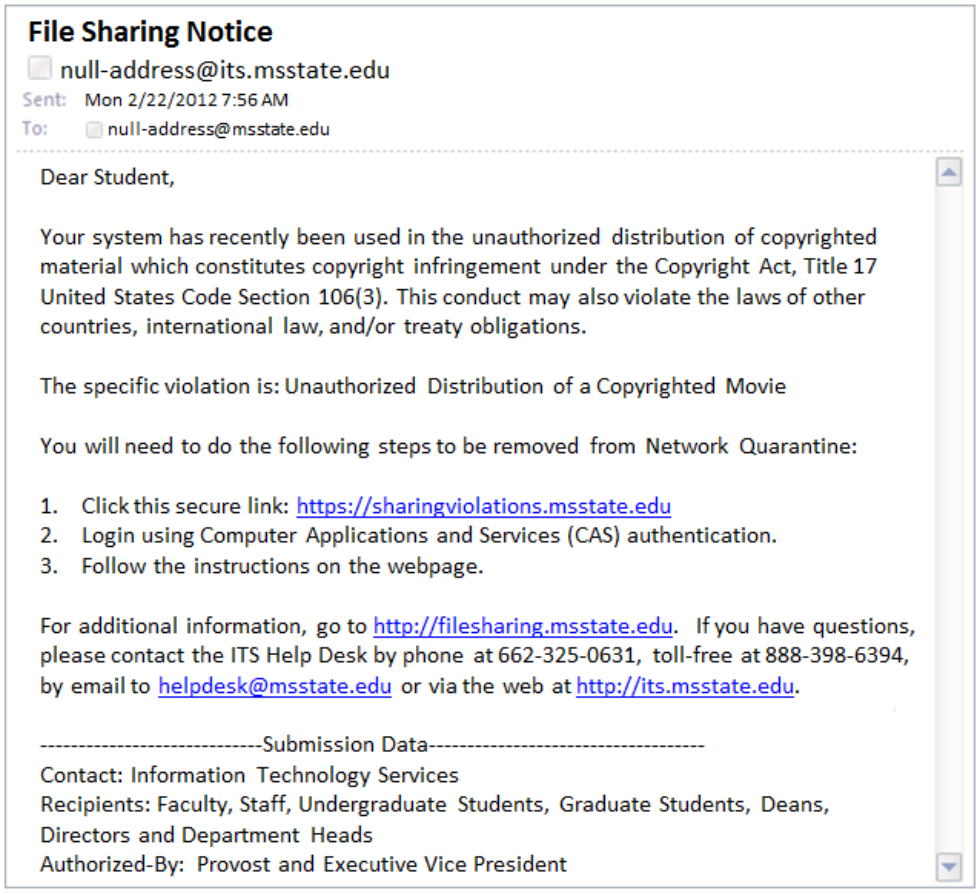


Figure 3: High Quality - High Quantity Message



File Sharing Notice

null-address@its.msstate.edu

Sent: Mon 2/22/2012 7:56 AM

To: null-address@msstate.edu

Dear Student,

Your system has recently been used in the unauthorized distribution of copyrighted material which constitutes copyright infringement under the Copyright Act, Title 17 United States Code Section 106(3). This conduct may also violate the laws of other countries, international law, and/or treaty obligations.

The specific violation is: Unauthorized Distribution of a Copyrighted Movie

You will need to do the following steps to be removed from Network Quarantine:

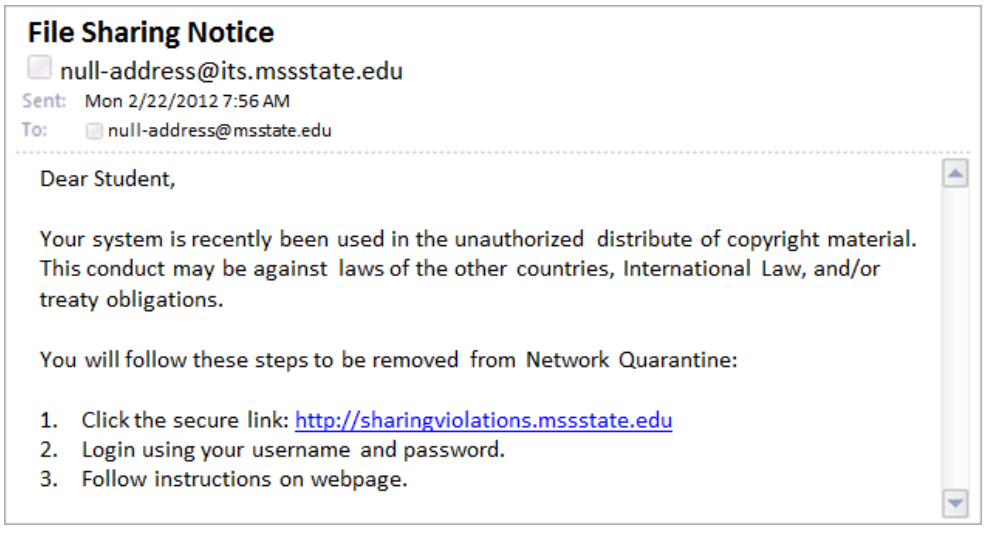
1. Click this secure link: https://sharingviolations.msstate.edu
2. Login using Computer Applications and Services (CAS) authentication.
3. Follow the instructions on the webpage.

For additional information, go to http://filesharing.msstate.edu. If you have questions, please contact the ITS Help Desk by phone at 662-325-0631, toll-free at 888-398-6394, by email to helpdesk@msstate.edu or via the web at http://its.msstate.edu.

----------Submission Data----------

Contact: Information Technology Services
Recipients: Faculty, Staff, Undergraduate Students, Graduate Students, Deans, Directors and Department Heads
Authorized-By: Provost and Executive Vice President

Figure 4: Low Quality - Low Quantity Message



File Sharing Notice

null-address@its.mssstate.edu

Sent: Mon 2/22/2012 7:56 AM

To: null-address@msstate.edu

Dear Student,

Your system is recently been used in the unauthorized distribute of copyright material. This conduct may be against laws of the other countries, International Law, and/or treaty obligations.

You will follow these steps to be removed from Network Quarantine:

1. Click the secure link: http://sharingviolations.mssstate.edu
2. Login using your username and password.
3. Follow instructions on webpage.

Measures

In the present study, we measured nine constructs: message quantity (QT), message quality (QL), perceived message honesty (PH), perceived source competence (PC), third-party support (SUP),

direct experience (DE), technology anxiety (TA), truth bias (TB), and perceived message risk (PR). All measurements are multi-item scales adapted from previous research (see Appendix A) to fit the context of the present study. For our measurement of QT, QL, PH, and PC, we adapted 5-point semantic differential scales from McCornack (1992) and Berlo, Lemert, and Mertz (1969). For our measurement of SUP, DE, TA, TB, and PR we adapted previously validated multi-item scales based on fully anchored 5-point Likert scales. SUP was adapted from Sitren and Applegate (2007). DE was adapted from Jarvenpaa et al. (2000) and Boss et al. (2009). TA was adapted from Thatcher and Perrewé (2002), Kinard, Capella, & Kinard (2009), and Brown, Fuller, & Vician (2004). TB was adapted from Stiff, Kim, and Ramesh (1992) and Boyle (2003). PR was adapted from Featherman and Pavlou (2003).

DATA ANALYSIS AND RESULTS

The total number of respondents was 128 which yielded 122 complete responses. The online survey was created using Qualtrics where each respondent was presented with a screenshot portraying a different randomized scenario. Individual perceptions were evaluated based on 5-point Likert or semantic differential scales. We removed eight responses as response set – the tendency to respond to questions automatically and independent of the item content – was detected (Andrich, 1978; Kerlinger, 1973; Rennie, 1982); an instrument item asked participants to mark neutral which these individuals failed to mark. This left us with 114 usable responses. From the usable responses, 45% were male and 55% were female. Forty-five percent of participants were freshmen, 35% were sophomores, 20% were juniors, and 1% were seniors.

Instrument Validity

Data analysis was conducted using the partial least squares (PLS) method of model estimation through the use of SmartPLS (Ringle, Wende, & Will, 2005). PLS was first used to assess the measurement model for validity and reliability. For all variables, initial construct validity tests were conducted. We examined factor loadings to ensure they loaded cleanly on separate components without cross-loading (see Table 1). Preliminary analysis indicates unexpected cross-loading of some of our constructs, but our analysis will continue, and data quality issues may require that we collect more data as our next step.

Convergent validity, as defined by Campbell and Fiske (1959) and Loch, Straub, and Kamel (2003), is when items of the same construct should correlate at a significant level with each other. As indicated in Table 2, some (but not all) of our constructs displayed convergent validity as they had item loadings greater than 0.70 and AVE above 0.50 (Gefen & Straub, 2005). In addition, some (but not all) of our constructs displayed discriminant validity. Discriminant validity is confirmed by creating the square root of average variance explained (AVE) statistics and comparing them against correlation measures of other constructs (Loch et al., 2003). The square root AVE was greater than inter-construct correlations and item loadings were greater than the loadings on other constructs (see Table 2). Again, data quality issues and our sampling frame will be assessed to determine if another round of data collection is indicated.

Reliability

Initial reliability scores were obtained through reliability analysis. Composite reliability scores for the reflective variables are acceptable (greater than 0.70) for all constructs (Fornell & Larcker, 1981; Gefen & Straub, 2005).

Test of Model

Using PLS, we tested the structural model and associated hypotheses. Half of the ten hypotheses were supported as demonstrated in Table 3 and Figure 5. Additionally, we used the bootstrapping resampling procedure to determine path coefficients and explained variance for perceived message honesty, perceived source competence, and perceived message risk.

The quality and quantity of a message explain 25.2% of the variance in perceived source competence and 86.7% of the variance in perceived message honesty. H1a and H1b were not supported as the relationships between message quantity and perceived source competence and perceived message honesty were not significant. However, consistent with H2a and H2b, message quality had a significant positive effect on perceived source competence ($\beta = 0.319$, $p < 0.025$) and perceived message honesty ($\beta = 0.882$, $p < 0.005$).

Perceived message honesty, perceived source competence, third-party support, direct experience, technology anxiety, and truth bias explain 51.3% of the variance in perceived message risk. H3, H6, and H8 were not supported as the respective relationships between perceived source competence, direct experience, truth bias and perceived message risk were not significant. However, H4, H5, and H7 were significant as perceived message honesty ($\beta = -0.613$, $p < 0.005$), third-party support ($\beta = 0.228$, $p < 0.05$), and technology anxiety ($\beta = 0.150$, $p < 0.10$) had a significant effect on perceived message risk.

Table 1: Loadings, Cross-Loadings, and AVEs for Multi-Item Constructs

	QT	QL	PH	PC	TA	TB	SUP	DE	PR	AVE
QT1	0.811	0.664	0.651	0.382	0.006	0.068	-0.071	0.179	-0.584	0.633
QT2	0.832	0.764	0.721	0.478	-0.078	0.191	0.078	0.218	-0.544	
QT3	0.782	0.647	0.624	0.336	-0.090	0.143	0.133	0.170	-0.485	
QT4	0.755	0.627	0.563	0.284	-0.020	0.106	0.238	0.183	-0.407	
QL1	0.791	0.908	0.822	0.442	0.044	0.182	0.075	0.150	-0.588	0.833
QL2	0.731	0.875	0.795	0.376	-0.068	0.300	0.204	0.086	-0.562	
QL3	0.804	0.929	0.887	0.445	-0.077	0.204	0.098	0.221	-0.651	
QL4	0.788	0.938	0.888	0.520	-0.093	0.088	0.055	0.191	-0.615	
PH1	0.770	0.876	0.939	0.440	-0.136	0.249	0.045	0.144	-0.672	0.826
PH2	0.743	0.875	0.927	0.457	-0.069	0.209	0.135	0.201	-0.625	
PH3	0.740	0.852	0.888	0.376	-0.074	0.149	0.136	0.131	-0.596	
PH4	0.686	0.774	0.881	0.373	-0.107	0.226	0.136	0.120	-0.540	
PC1	0.448	0.470	0.428	0.916	0.078	0.074	0.052	0.097	-0.351	0.817
PC2	0.376	0.400	0.346	0.874	0.040	0.123	0.119	0.156	-0.242	
PC3	0.451	0.436	0.409	0.916	-0.028	0.123	0.046	0.119	-0.422	
PC4	0.427	0.462	0.449	0.908	0.004	0.164	0.030	0.014	-0.350	
TA1	-0.029	-0.020	-0.081	-0.010	0.665	-0.201	-0.102	0.202	0.176	0.639
TA2	0.109	0.142	0.085	0.123	0.708	-0.135	-0.236	0.336	0.056	
TA3	-0.086	-0.111	-0.125	-0.002	0.851	0.006	-0.190	0.124	0.167	
TA4	-0.112	-0.097	-0.165	0.000	0.802	-0.084	-0.186	0.179	0.096	
TA5	0.007	-0.006	-0.057	0.056	0.877	-0.078	-0.206	0.254	0.085	
TA6	-0.081	-0.055	-0.062	0.034	0.870	-0.061	-0.212	0.153	0.103	
TB1	0.192	0.230	0.258	0.135	-0.098	0.970	0.341	-0.087	-0.182	0.664
TB2	0.041	0.109	0.086	0.118	-0.070	0.663	0.288	-0.084	-0.055	
TB3	0.060	0.067	0.103	0.035	-0.174	0.782	0.410	-0.108	-0.039	
SUP1	0.099	0.079	0.093	-0.010	-0.145	0.425	0.678	-0.128	0.043	0.743
SUP2	0.126	0.126	0.138	0.104	-0.240	0.302	0.919	-0.094	0.040	
SUP3	0.085	0.102	0.105	0.067	-0.202	0.325	0.962	-0.162	0.107	
DE1	0.219	0.172	0.149	0.099	0.179	-0.061	-0.095	0.944	-0.102	0.833
DE2	0.252	0.188	0.168	0.142	0.355	-0.080	-0.120	0.859	-0.065	
DE3	0.240	0.186	0.170	0.121	0.217	-0.112	-0.177	0.954	-0.159	
DE4	0.162	0.116	0.117	0.021	0.185	-0.107	-0.163	0.890	-0.099	
PR1	-0.592	-0.584	-0.576	-0.415	0.134	-0.148	0.109	-0.153	0.934	0.897
PR2	-0.620	-0.678	-0.686	-0.374	0.172	-0.140	0.026	-0.082	0.948	
PR3	-0.605	-0.617	-0.642	-0.305	0.161	-0.151	0.118	-0.129	0.958	

Table 2: Inter-Construct Correlations

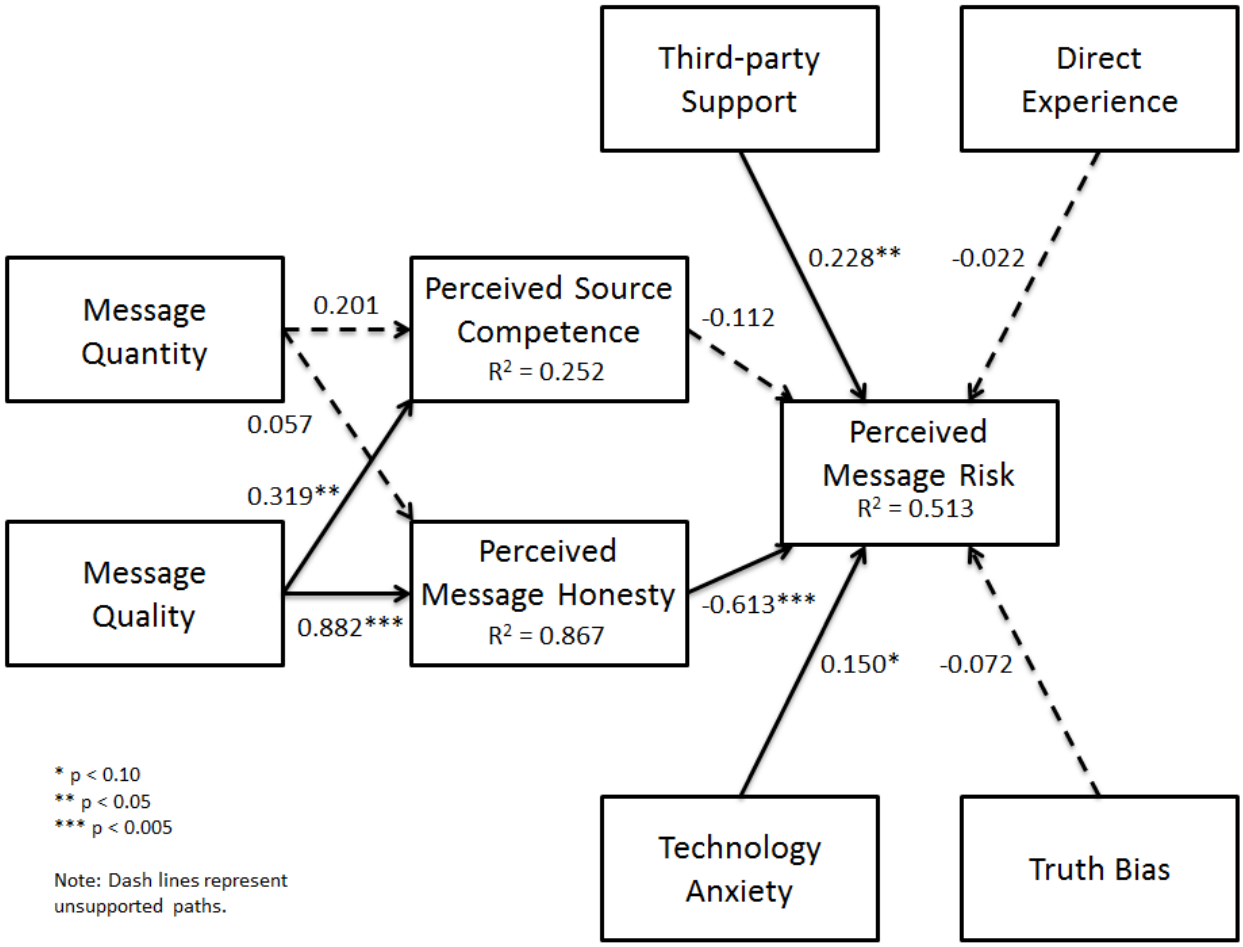
Construct	QT	QL	PH	PC	TA	TB	SUP	DE	PR
QT	**0.795**								
QL	0.854	**0.913**							
PH	0.810	0.930	**0.909**						
PC	0.473	0.491	0.454	**0.904**					
TA	-0.059	-0.055	-0.106	0.024	**0.800**				
TB	0.162	0.207	0.229	0.133	-0.117	**0.815**			
SUP	0.109	0.115	0.123	0.065	-0.222	0.386	**0.862**		
DE	0.237	0.180	0.165	0.104	0.240	-0.102	-0.158	**0.913**	
PR	-0.640	-0.663	-0.672	-0.384	0.165	-0.154	0.088	-0.127	**0.947**

Shaded items are square root of average variance extracted (AVE)

Table 3: Overview of Findings

Hypothesis & Direction	Path Coefficient (β)	T Value	P-value	Supported?
H_{1a}: QT → PC (+)	0.201	1.198	$p < 0.10$	Unsupported
H_{1b}: QT → PH (+)	0.057	0.813	$p < 0.10$	Unsupported
H_{2a}: QL → PC (+)	0.319	2.311	$p < 0.025$	Supported
H_{2b}: QL → PH (+)	0.882	13.986	$p < 0.005$	Supported
H_3: PC → PR (-)	-0.112	1.161	$p < 0.10$	Unsupported
H_4: PH → PR (-)	-0.613	6.387	$p < 0.005$	Supported
H_5: SUP → PR (+)	0.228	1.763	$p < 0.05$	Supported
H_6: DE → PR (+)	-0.022	0.253	$p < 0.10$	Unsupported
H_7: TA → PR (+)	0.150	1.560	$p < 0.10$	Supported
H_8: TB → PR (-)	-0.072	0.685	$p < 0.10$	Unsupported

Figure 5: Results of PLS Structural Model Analysis



DISCUSSION AND CONTRIBUTION

Message quantity may be insignificant because messages can only be evaluated based on the information available. For most individuals, identifying missing information is complex and may require extensive involvement. Considering that phishing and other deceptive messages are presented once, the lack of background and additional details may hinder an individual's ability to judge that a message has complete information. In addition, individuals tend to compare messages against baseline messages. In the circumstance where only one message is presented, individuals lack information a baseline message provides; therefore, they would not recognize missing or additional information because they have no alternative to compare against.

Surprisingly, the relationship between direct experience and perceived message risk was insignificant. This may be because risk cues in previous messages may be different based on the message. Therefore, having direct experience with one aspect of a message may not be helpful in identifying future messages as risky.

In digital communication, truth bias may virtually be obsolete. With access to time, tools, and others, individuals can make a more informed response to messages that may be risky. Just as deceivers have time to craft and rehearse their messages, receivers can spend time rereading and analyzing a message, searching the internet for similar messages, or asking others about their perceptions. The combination of these factors may override an individual's truth bias.

This study contributes to the fields of information systems, specifically security and deception, by applying IMT to a digital setting. The impact of message quality and perceived honesty significantly affects message risk in digital communications. In addition, this model shows how third-party support and technology anxiety affect perceived risk.

Because technology anxiety has a positive effect on perceived message risk, companies should focus on reducing technology anxiety for its employees to ensure they adhere to valid messages only. Through proper training and support, employees will be able to better distinguish between risky and valid messages and follow recommended responses for each message.

Considering that third-party support increases perceptions of message risk, corporations should facilitate learning, cohesion, and cooperation among employees. Under these conditions, employees who encounter potentially risky messages can reach out for support from coworkers and management before making decisions. This help from others can help ensure the safety of company information. In addition, training users to recognize proper assurance mechanisms can help users distinguish between valid and deceptive messages.

Since the quality of a message strongly influences individual perceptions of honesty, valid messages should be carefully created so they are not rejected. In addition, companies should discuss with their employees the key aspects of low quality messages to provide the tools for employees to recognize the difference between valid and risky messages. Since higher perceptions of honesty reduce perceived message risk, companies should ensure that users perceive valid messages as honest and deceptive messages as dishonest.

LIMITATIONS AND FUTURE RESEARCH

One limitation is the method of data collection. Survey research has high generalizability as questionnaires can be distributed across multiple industries to people with varying demographics. However, this research method lacks realism because the survey is created by the researcher (introducing researcher bias) and asks specific questions (restricting user response). Also, survey research lacks precision as individuals respond under various conditions introducing additional extraneous variables. Additional methods for collecting data can be explored to further validate this model.

Another limitation is that this research evaluates perception of honesty, competence, and risk. Although these constructs have been used extensively in previous literature, perceptions are self-reported measures and may not indicate actual measures. An individual's perceptions may be completely opposite. For example, a user may view a message as honest, but the same message may be created to deceive.

An additional limitation may be the age of our subjects. Since the majority of our subjects were between 18 and 25, this may affect the generalizability of this study. However, the exact ramifications on generalizability are unclear.

Finally, IMT looks at four manipulations of messages: quantity, quality, relation, and manner. In this study, we evaluated only two of these maxims. Future research could examine the other maxims and their effects on digital messages. Also, these messages may be evaluated in different contexts such as email conversations or chat messages.

CONCLUSIONS

This paper evaluated the impact IMT has on perceived message risk, specifically the role of message quantity and message quantity. Through this study, we have determined that the quality of a message has a greater impact than the quantity of a message on whether an individual perceives a message to be honest which ultimate leads to individual perceptions of risk. In addition, technology anxiety and third-party support affect perceptions of risk. Therefore, the present study stresses the need for corporations to help their users recognize low quality messages. Also, by ensuring support is available, individuals are less likely to follow risky messages. Lastly, this research suggests that individuals who experience higher levels of technology anxiety are more likely to perceived messages as risky which may lead to valid messages being rejected.

REFERENCES

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior* (pp. 1-278). Engelwood Cliffs, NJ: Prentice-Hall.

Anderson, R. (2008). *Security engineering* (2nd ed.). New York, NY: John Wiley & Sons.

Andrich, D. (1978). A rating formulation for ordered response categories. *Psychometrika*, *43*(4), 561-573.

Berlo, D. K., & Lemert, J. B. (1961). A factor analytic study of the dimensions of source credibility. *SAA Conference*. New York, NY.

Berlo, D. K., Lemert, J. B., & Mertz, R. J. (1969). Dimensions for evaluating the acceptability of message sources. *The Public Opinion Quarterly*, *33*(4), 563-576.

Boss, S. R., Kirsch, L. J., Angermeier, I., & Boss, R. W. (2009). Familiarity breeds content: How fear of cybercrime influences individual precaution-taking behavior. *IFIP TC8 International Workshop on IS Security Research* (pp. 24-53). Capetown, South Africa.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, *18*, 151-164.

Boyle, R. J. (2003). *Dispersed deception: An examination of the impacts of computer mediation, proximity, and familiarity on truth bias*. The Florida State University, Tallahassee, FL.

Brown, S. A., Fuller, R. M., & Vician, C. (2004). Who's afraid of the virtual world? Anxiety and computer-mediated communication. *Journal of the Association for Information Systems*, *5*(2), 79-107.

Buller, D. B., & Burgoon, J. K. (1996). Interpersonal deception theory. *Communication Theory*, *6*(3), 203-242.

Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin*, *56*(2), 81-105.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61-80.

Dolan, A. (2004). *Social engineering*. *Information Security* (pp. 1-16). Retrieved from http://www.sans.org/reading_room/whitepapers/engineering/social-engineering_1365

Dowling, G. R., & Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. *Journal of Consumer Research*, *21*, 119-134.

Enrici, I., Ancilli, M., & Lioy, A. (2010). A psychological approach to information technology security. *3rd International Conference on Human System Interaction* (pp. 459-466). Rzeszow, Poland.

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

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*, 39-50.

Gefen, D., & Straub, D. W. (2005). A practical guide to factorial validity using PLS-graph: Tutorial and annotated example. *Communications of the Association for Information Systems*, *16*, 91-109.

George, J. F., & Robb, A. (2008). Deception and computer-mediated communication in daily life. *Communication Reports*, *21*(2), 92-103.

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: Systems and Humans*, *30*(4), 395-410.

Grice, P. (1989). *Studies in the way of words* (pp. 1-395). Cambridge, MA: Harvard University Press.

Hachman, M. (2012). Anonymous: Symantec offered $50K for stolen code, plus a lie. *PC Magazine*. Retrieved March 2, 2012, from http://www.pcmag.com/article2/0,2817,2399912,00.asp

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an internet store. *Information Technology and Management*, *1*, 45-71.

Kerlinger, F. N. (1973). *Foundations of Behavioral Research* (2nd ed.). London, UK: Holt Reinhart & Winston.

Kinard, B. R., Capella, M. L., & Kinard, J. L. (2009). The impact of social presence on technology based self-service use: The role of familiarity. *Services Marketing Quarterly*, *30*(3), 303-314.

King, R. C., & Xia, W. (1997). Media appropriateness: Effects of experience on communication media choice. *Decision Sciences*, *28*(4), 877-910.

Loch, K. D., Straub, D. W., & Kamel, S. (2003). Diffusing the Internet in the Arab world: The role of social norms and technological culturation. *IEEE Transactions on Engineering Management*, *50*(1), 45-63.

Marakas, G. M., Yi, M. Y., & Johnson, R. D. (1998). The multilevel and multifaceted character of computer self-efficacy: Toward clarification of the construct and an integrative framework for research. *Information Systems Research, 9*(2), 126-163.

McCornack, S. A. (1992). Information manipulation theory. *Communication Monographs, 59*(March), 1-16.

McCornack, S. A., Levine, T. R., Solowczuk, K. A., Torres, H. I., & Campbell, D. M. (1992). When the alteration of information is viewed as deception: An empirical test of Information Manipulation Theory. *Communication Monographs, 59*(March), 17-29.

Park, H. S., Levine, T. R., McCornack, S. A., Morrison, K., & Ferrara, M. (2002). How people really detect lies. *Communication Monographs, 69*(2), 144-157.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the Technology Acceptance Model. *International Journal of Electronic Commerce, 7*(3), 101-134.

Pornpitakpan, C. (2004). The persuasiveness of source credibility: A critical review of five decades' evidence. *Journal of Applied Social Psychology, 34*(2), 243-281.

Rennie, L. J. (1982). Research note: Detecting a response set to likert-style attitude items with the rating model. *Education Research and Perspectives, 9*(1), 114-118. Retrieved from http://204.202.14.77/erp9.htm

Ringle, C. M., Wende, S., & Will, S. (2005). SmartPLS 2.0 (M3) Beta. Hamburg, Germany. Retrieved from http://www.smartpls.de

Sitren, A. H., & Applegate, B. K. (2007). Testing the deterrent effects of personal and vicarious experience with punishment and punishment avoidance. *Deviant Behavior, 28*(1), 29-55.

Stiff, J. B., Kim, H. J., & Ramesh, C. N. (1992). Truth biases and aroused suspicion in relational deception. *Communication Research, 19*(3), 326-345.

Taylor, S., & Todd, P. (1995). Assessing IT usage: The role of prior experience. *MIS Quarterly, 19*(4), 561-570.

Thatcher, J. B., & Perrewé, P. L. (2002). An empirical examination of individual traits as antecedents to computer anxiety and computer self-efficacy. *MIS Quarterly, 26*(4), 381-396.

Appendix A: Origination of Scale Items for Research Constructs

Construct	Adapted Scale Items	Original Scale Items	Source
Message Quantity (QT)	1. Uninformative---Informative 2. Incomplete---Complete 3. Nondisclosive---Disclosive 4. Concealing---Revealing	1. Uninformative---Formative 2. Incomplete---Complete 3. Nondisclosive---Disclosive 4. Concealing---Revealing	McCornack et al. (1992)
Message Quality (QL)	1. Distorted---Accurate 2. Altered---Authentic 3. Fabricated---Genuine 4. False---True	1. Distorted---Accurate 2. Altered---Authentic 3. Fabricated---Genuine 4. False---True	McCornack et al. (1992)
Perceived Message Honesty (PH)	1. Dishonest---Honest 2. Deceitful---Truthful 3. Deceptive---Not Deceptive 4. Misleading---Not Misleading	1. Dishonest---Honest 2. Deceitful---Truthful 3. Deceptive---Not Deceptive 4. Misleading---Not Misleading	McCornack et al. (1992)
Perceived Source Competence (PC)	1. Ineffective---Effective 2. Inept---Skillful 3. Incompetent---Competent 4. Mismanaged---Well-managed 5. Incapable---Capable	1. Ineffective---Effective 2. Inept---Skillful 3. Incompetent---Competent 4. Mismanaged---Well-managed 5. Incapable---Capable	McCornack et al. (1992) and Berlo, Lemert, and Mertz (1969)
Third-party Support (SUP)	1. When I am unsure about computers, I can talk to my friends or coworkers. 2. I know people I can go to for advice about computers. 3. I know others I can talk to when I need advice about computers.	1. When I have a bad day, I can talk to my friends. 2. I don't know anyone I can go to for advice (R). 3. I can talk to my parents when I need advice.	Sitren and Applegate (2007)
Direct Experience (DE)	1. I frequently receive emails from unknown sources requesting my personal information. 2. I frequently receive emails from unknown sources asking for my username and password. 3. I frequently receive email messages from unknown sources requesting sensitive information.	1. I frequently buy products through television shopping channels. 2. I frequently watch infomercials on television. 3. I frequently buy products from printed catalogs. 4. Downloading a file that is infected with a virus through my e-mail.	Jarvenpaa et al. (2000) Boss et al. (2009)

	4. I frequently receive email messages from unknown sources asking me to take a specific course of action.		
Technology Anxiety (TA)	1. I feel apprehensive about using computers. 2. I hesitate using a computer for fear of making mistakes. 3. Computers are somewhat intimidating to me. 4. I usually avoid using computers because they are unfamiliar to me. 5. Computers make me feel uncomfortable. 6. Working with a computer makes me nervous.	1. I feel apprehensive about using computers. 2. I hesitate to use a computer for fear of making mistakes that I cannot correct. 3. Computers are somewhat intimidating to me. 4. I usually avoid new technology because it is unfamiliar to me. 5. Computers make me feel uncomfortable. 6. Working with a computer makes me nervous.	Thatcher and Perrewé (2002) Kinard, Capella, and Kinard (2009) Brown, Fuller, and Vician (2004)
Truth Bias (TB)	1. I think email messages I receive from MSU are generally honest. 2. I rarely doubt email messages I receive from MSU. 3. Overall, email messages I receive from MSU are truthful.	1. I think my relational partner is generally honest. 2. I believe what my partner says with little doubt. 3. Overall, my partner was truthful. 4. Overall, my partner was very deceptive (R).	Stiff, Kim, and Ramesh (1992) Boyle (2003)
Perceived Message Risk (PR)	1. Clicking the recommended link in the email could be harmful. 2. Clicking the recommended link in the email is dangerous. 3. Clicking the recommended link in the email exposes me to risk.	1. On the whole, considering all sorts of factors combined, about how risky would you say it would be to sign up for and use XXXX? 2. Using XXXX to pay my bills would be risky. 3. XXXX are dangerous to use. 4. Using XXXX exposes you to an overall risk.	Featherman and Pavlou (2003)