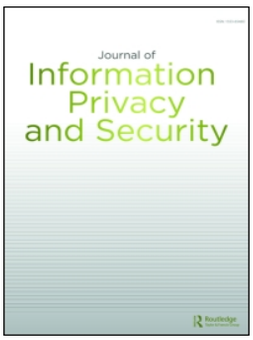

Routledge
Taylor & Francis Group

Journal of Information Privacy and Security

ISSN: 1553-6548 (Print) 2333-696X (Online) Journal homepage: http://www.tandfonline.com/loi/uips20

Perceived deception: Evaluating source credibility and self-efficacy

Dustin Ormond, Merrill Warkentin, Allen C. Johnston & Samuel C. Thompson

To cite this article: Dustin Ormond, Merrill Warkentin, Allen C. Johnston & Samuel C. Thompson (2016) Perceived deception: Evaluating source credibility and self-efficacy, Journal of Information Privacy and Security, 12:4, 197-217, DOI: 10.1080/15536548.2016.1243857

To link to this article: http://dx.doi.org/10.1080/15536548.2016.1243857

JOURNAL OF INFORMATION PRIVACY AND SECURITY
2016, VOL. 12, NO. 4, 197–217
http://dx.doi.org/10.1080/15536548.2016.1243857

Routledge
Taylor & Francis Group

ARTICLE

Perceived deception: Evaluating source credibility and self-efficacy

Dustin Ormond [a], Merrill Warkentin [b], Allen C. Johnston [c], and Samuel C. Thompson [c]

[a]Creighton University; [b]Mississippi State University; [c]University of Alabama at Birmington

ABSTRACT

Detecting scareware messages that seek to deceive users with fear-inducing words and images is critical to protect users from sharing their identity information, money, and/or time with bad actors. Through a scenario-based experiment, the present study evaluated factors that aid users in perceiving deceptive communications. An online experiment was administered yielding 213 usable responses. The data from the study indicate high levels of deception detection self-efficacy and source trustworthiness increase the likelihood an individual will perceive a scareware message as deceptive. Additionally, technology awareness enhances self-efficacy to detect deception and reduces individual perceptions of source trustworthiness. Finally, the data significantly illustrate behavioral intention to use scareware is lower when the message is perceived as deceptive.

Introduction

As the world of computing continues to develop, information security and privacy are increasingly a global concern. One particularly troublesome threat to global information security and privacy is *scareware*, malware that engenders fear in victims with nonexistent threats by displaying false alert messages (Sophos, 2010). Rogue security software (scareware) masquerades as genuine security software such as flash updates (Zorz, 2016), while in actuality reporting incorrect results of simulated malware scans or enticing users to install fake anti-virus software (Butler, 2016). To further increase user trust, scareware perpetrators adopt convincing names to add to the illusion of legitimacy, such as "AntiSpyWarePro, Antivirus Plus, Malware Defense, and CleanUp AntiVirus" (Sophos, 2010). Early scareware varieties were often inundated with misspellings, poorly designed graphical user interfaces, and lack of security seals. However, the more modern scareware instantiations are not as mistake prone as they once were and are increasingly more like their legitimate counterparts (Butler, 2016; Sophos, 2011a). Recent scareware was introduced into Google Play apps by circumventing initial scans by Google through delaying scareware messages until 2 days after installation (Constantin, 2015).

Scareware may be created for the sole purpose of capturing users' personal information or infecting personal/business computers. For example, scareware may entice its victims to pay for fake threat removal tools (Sophos, 2011b) only to capture their sensitive bank account information. Crimes associated with scareware are increasing as criminals understand they are very lucrative ventures (Stone-Gross et al., 2011). In some cases, the sale of unnecessary virus removal software ("Fake AV") is very lucrative, especially when the target audience is so large. One example of this deception was found in a popular Facebook game called Farm Town, which had more than 9.6 million players at the time. Although Farm Town appeared to be a free game, the developers charged advertisers to display ads within the game as pop-ups. One such pop-up purported to warn Farm Town users about the possibility of receiving malware. Advertisements would popup fake security warnings that would encourage people to pay for unnecessary anti-virus software (Mills, 2010).

CONTACT Merrill Warkentin m.warkentin@msstate.edu Department of Management & Info Systems, College of Business, Mississippi State University, Mississippi State, MS 39762-9581, USA.

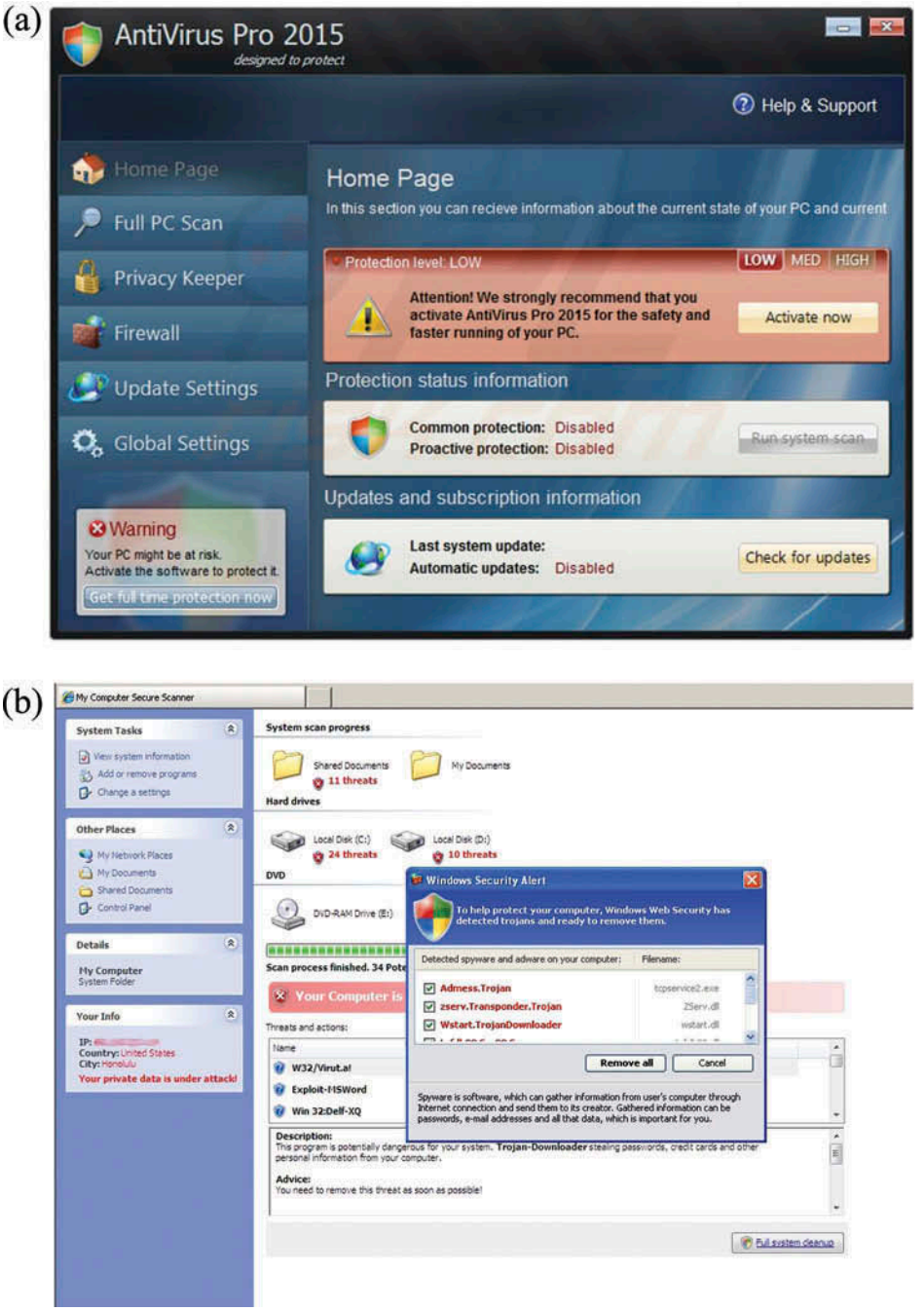

Figure 1. (a) Example of scareware—AntiVirus Pro 2015; (b) example of scareware—Windows security alert.

The focus of this study is on educating users of the danger associated with scareware messages. Figure 1a illustrates an example of scareware, AntiVirus Pro 2015 which seeks to deceive users while providing no protection in exchange for the actual money they pay for it. Figure 1b displays another rogue security software that mimics a Windows message. Because fake security software is approximately 15% of all malware on the web (Martinez-Cabrera & Kim, 2010) and is increasingly growing,

business/home users are likely to encounter these threats. Related threats, malvertising and fake browser updates or Adobe updates, utilize similar deceitful messages to scam users into downloading malware, manipulating victims with fear that their software is out of date and needs updating (Larsen, 2011, 2013). The increased probability of exposure increases the likelihood of a misguided user being infected. Scareware on business systems is very problematic as it may introduce a back door that can be used to capture confidential information, alter business data, or take down vital business systems. Such infected business systems may result in millions of dollars in losses or may cause businesses to cease operations altogether due to their customers' inability to transact, the business's need to recover data, and/or their trade secrets being publicized.

In order to avoid succumbing to attacks like the scareware just described, it is incumbent upon Internet users to perceive an element of deceptive intent behind the unexpected message. In the "bait and hook" metaphor used to describe phishing attacks (Wright & Marett, 2010), users are first presented with an email message (the "bait") encouraging them to follow an embedded link to a bogus Web site (the "hook") soliciting account information from them. Similarly, attention-grabbing scareware messages attempt to direct users to download a bogus virus scanning application. By the time users have made the decision to proceed with the download, the "hook" is almost guaranteed to be set. Indeed, the point at which scareware recipients may be able to circumvent the scam is when initially receiving the message.

Scareware message recipients may become suspicious of the message's veracity and may perceive deception only if certain factors associated with the message are inconsistent with the level of communication expected from its source (Grazioli, 2004; Wright, Chakraborty, Basoglu, & Marett, 2009). However, it is unclear as to which factors lead to suspicion and the degree to which they are able to influence the receivers to avoid potentially harmful software. The following research questions guide the remainder of this study:

- What factors impact an Internet user's ability to perceive deception and reject computer security threats?
- What enhances these factors and indirectly reduces the likelihood of succumbing to deception?

To answer these research questions, we look at the underlying premise of scareware, the betrayal of trust and the inability of the recipient to readily and reliably detect its deception; a digital proxy of social engineering. Unfortunately, no previous research has explored scareware and the set of recipient perceptions that shape one's ability to detect deception and avoid harmful exposure. This study serves as an initial exploration toward a better understanding of this phenomenon. Our findings may serve as a first step in describing how scareware recipients formulate their detection of deception and, ultimately, their intentions to avoid its dangerous payload. First, we present a review of the extant literature focused in this area, followed by our research model with the corresponding hypotheses and supporting literature. Next, we discuss our research method, analysis, and results. Finally, we end with study implications and contributions as well as the limitations of our study.

Literature review

Individual computer users must frequently and quickly make decisions regarding actions to take when online such as clicking a link in an email, responding to a pop-up, or confirming a suggested procedure or other requested action. Unfortunately, deception is an integral part of today's reality in the online world, and poor choices can lead to devastating consequences. *Deception* is defined as "a message knowingly transmitted by a sender to foster a false belief or conclusion by the receiver" (Buller & Burgoon, 1996). Grazioli and Jarvenpaa (2000) further define *Internet deception* as "the malicious manipulation of information presented on the Internet for the purpose of inducing online users to act in ways that unfairly benefit the provider of the manipulated information." Deception is

a prevalent technique for various social engineering attacks, such as by phishing and "spear phishing" attacks (Fuller, Marett, & Twitchell, 2012; Wright & Marett, 2010), and by manipulating the following:

- online employment recruitment (Allen, Mahto, & Otondo, 2007),
- social media relationships (Alowibdi, Buy, Yu, Ghani, & Mokbel, 2015; Hancock, Toma, & Ellison, 2007; Hancock, Woodworth, & Goorha, 2010; Kaplan & Haenlein, 2011; Zhou, Burgoon, Twitchell, Qin, & Nunamaker, 2004),
- electronic commerce (Pennington, Wilcox, & Grover, 2004; Wang & Benbasat, 2007),
- gender (Ho, Lowry, Warkentin, Yang, & Hollister, 2016),
- insider abuse (Ho & Warkentin, 2015), and
- professional virtual communities (Joinson & Dietz-Uhler, 2002).

Users must be able to recognize online deception to maximize their online safety and to avoid fraud, data loss, identity theft, and other undesirable outcomes. Considering that people correctly identify deception only 54% of the time (Bond & DePaulo, 2006; Vrij, 2001) and that approximately 30% of people admit to engaging in online deception (Alowibdi et al., 2015; Caspi & Gorsky, 2006), deceptive communication across digital media is definitely a concern. Deception is often associated with lying, however, it includes other deceptive behaviors such as selectivity, oversimplification, or the omission of information (Burgoon, Buller, Ebesu, & Rockwell, 1994; Miller & Stiff, 1993). Additionally, deception is found in 20% to 25% of all communication (George & Robb, 2008).

Determining the credibility of deceptive messages has resulted in tremendous costs to businesses and society (Jensen, Lowry, & Jenkins, 2011). Decision aids have been implemented and improved overall credibility assessment (Warkentin & Johnston, 2006a); however, both novices and professionals often discount the recommendations in these decision aids, especially when in conflict with their own assessments (Jensen, Lowry, Burgoon, & Nunamaker, 2010; Jensen et al., 2011). Deviant software such as scareware play on this conflict to entice users to engage in security behavior that is contrary to what is expected. Persuasive influences and strategies incorporated into deviant software have shown to have more successful attempts (Ebot & Siponen, 2014; Jones, Towse, & Race, 2015). Given that the standard method used by scareware developers involves a realistic-looking scan of an Internet user's computer with the purpose of instilling a sense of vulnerability in the user, it is reasonable to infer the intent of a scareware message is to deceive.

Understanding the factors that users consider when evaluating the deceptiveness of a message is instrumental to protect against unintentional negative consequences for the individual or business. Our research study extends prior research in deceptive communication by examining individual and source factors that both directly and indirectly influence user perception about the deceptiveness of messages and ultimately behavioral intention with regard to these messages. These factors include the impact of source trustworthiness, individual deception detection self-efficacy, and individual technology awareness.

Conceptual model and hypotheses development

We reviewed the extant literature on detecting computer-mediated deceptive communication to identify factors that cause an Internet user to perceive a message as deceptive, as in the case of scareware. Because of the aforementioned similarities between the phishing "bait" and scareware "scan alert," previous work on detecting phishing was pertinent. Factors influencing the detection of phishing deception have been observed to be a mixture of perceptual, dispositional, and experiential variables (Dhamija, Tygar, & Hearst, 2006; Wright & Marett, 2010). Thus, we developed a model for the current study that extends beyond models provided by Wright and Marett (2010), Miller and Stiff (1993), and Carlson and George (2004). Our conceptual model (see Figure 2) accounts for

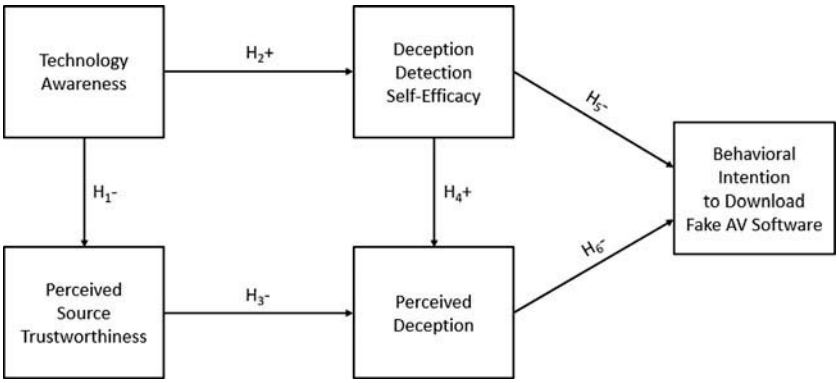

Figure 2. Conceptual model.

Table 1. Construct definitions.

Construct	Definition	Source
Technology Awareness	A user's raised consciousness of and interest in knowing about technological issues and strategies to deal with them.	Dinev and Hu (2007)
Perceived Source Trustworthiness	The degree to which an Internet user believes a communicator's message as being valid and that the message source is motivated to provide accurate information.	Hovland, Janis, and Kelley (1953), Kelman and Hovland (1953)
Deception Detection Self-Efficacy	An Internet user's perceptions of his or her own ability to identify a source or message as misleading.	Adapted for this study from Bandura (1977).
Perceived Deception	The extent to which an Internet user interprets a message source, message meaning, or message intention to be different than what it is purported to be.	Developed for this study.
Behavioral Intention	The indication of an Internet user's readiness to perform a given behavior.	Ajzen and Fishbein (1980), Fishbein and Ajzen (1975)

Internet users' technology awareness, trustworthy assessment about the source of the message, and deception detection self-efficacy. Constructs that are included in this model are defined in Table 1.

Awareness is defined as "the extent to which a target population is conscious of an innovation and formulates a general perception of what it entails" (Dinev & Hu, 2007). Previous studies (Goodhue & Straub, 1991) state that awareness arouses concern about the security and perceptions of an existing environment. Security awareness is also known to be positively correlated with security practice (Chen, Schmidt, Phan, & Arnett, 2008). In essence, the more aware an individual is of current issues in security, the more concern that he or she will have about security. Additionally, risk awareness leads to a loss in trust (Olivero & Lunt, 2004). Also, awareness is considered an essential ingredient for garnering trust towards online websites, meaning that a website needs to earn trust to be an effective site (Yoon, 2002). Dinev and Hu (2007) further state that technological awareness influences the need for defending against security threats originating from negative technologies. Individual technology awareness is increased through activities such as staying up-to-date on existing technologies or issues, communicating with coworkers or colleagues about certain technologies, etc. Jones et al. (2015) further demonstrate that general awareness is a factor that influences trustworthiness. Based on this rationale, we form the following hypothesis:

- H1: Technology awareness negatively influences perceived source trustworthiness.

In addition to examining the impact of technology awareness on source trustworthiness, this study extends the prior discussion of technology awareness in the context of deception detection self-efficacy. An awareness of the communicative medium can boost a computer user's belief that, should

he or she be lied to across the medium, the attempted deception will be readily apparent. Following from channel expansion theory, users with a general understanding of how the medium works (its levels of synchronicity, cue multiplicity, language variety, etc.) will believe themselves to be better equipped at reprocessing the message and determining the veracity of a message (Carlson & George, 2004; Carlson & Zmud, 1999). Therefore, we hypothesize that:

- H2: Technology awareness positively influences deception detection self-efficacy.

For Internet users to perceive deception, they will appraise characteristics regarding message trustworthiness through a credibility assessment (Jensen et al., 2010). As an individual assesses a source to be more credible, he or she is less likely to detect deception (Marett & George, 2004). In the case of scareware, Internet users may not fully understand the potential security threats that exist and, therefore, become victims of these threats. For example, if a user browses a reputable website that has been hijacked, unbeknownst to him or her, the user may follow the recommendations of the implanted scareware because he or she trusts the company that operates the website. Extending the work of Berlo and Lemert (1961), we assess credibility by evaluating source trustworthiness.

Determining the trustworthiness of the message source is a critical factor in ensuring safety when engaging in online activity (Twyman, Lowry, Burgoon, & Nunamaker, 2014), and constitutes an important component of good security hygiene. *Trustworthiness* is a dimension of source credibility and is defined as the extent to which an individual perceives a source is communicating what it considers valid (Hovland & Weiss, 1951) and the source is determined to deliver accurate information (Kelman & Hovland, 1953). Factors that may increase source trustworthiness include level of authority, past history, and awareness of what to expect from the sender (Jones et al., 2015). For example, sources who appear to have higher authority (e.g., a scientific researcher) are deemed more trustworthy than sources with less authority (e.g., an undergraduate student). In general, arguments are accepted more from highly trustworthy sources than low trustworthy sources (Hovland & Weiss, 1951). Therefore, scareware effectively purporting to be trustworthy are less likely to be perceived as deceptive. We then posit that:

- H3: Perceived source trustworthiness negatively influences perceived deception.

Bandura (1995) defines *self-efficacy* as "the belief in one's capabilities to organize and execute the courses of action required to manage prospective situations," and he states that self-appraisals of one's capabilities often affect an individual's motivation and behavior (Bandura, 1982). In the context of using computers, self-efficacy is an individual judgment of one's capability to use a computer in many situations (Compeau & Higgins, 1995; Marakas, Yi, & Johnson, 1998). Based on prior research, we define *deception detection self-efficacy* as a user's belief in his or her capacity to recognize deceptive or misleading communication. As Vrij (2001) points out, a high degree of confidence in one's own ability to detect deception often leads to quick decisions about a message's veracity, and individuals with higher confidence are more likely to judge a message as deceptive than less confident people. It should be noted that a review of the deceptive communication literature does not indicate a strong relationship between an individual's confidence in his or her deception detection abilities and his or her detection accuracy (DePaulo, Charlton, Cooper, Lindsay, & Muhlenbruck, 1997; Granhag & Vrij, 2005). Nevertheless, we expect that individuals with relatively higher levels of deception detection self-efficacy will form stronger perceptions of message (or communication) deceptiveness, regardless of its veracity. Likewise, we anticipate that high levels of deception detection self-efficacy will influence intentions. As such, we formulate the following hypotheses:

- H4: Deception detection self-efficacy positively influences perceived deception.

- H5: Deception detection self-efficacy negatively influences behavioral intention to download anti-virus software.

The final hypothesis involves the behavioral intent resulting from the user perceiving deception in the message. In the context of this study, perceived deception is defined as the extent to which one interprets a message source, message meaning, or message intention to be deliberately different than what it is purported to be. This definition parallels previous measures of perceived deception used in other studies of online deceptive communication (Grazioli & Jarvenpaa, 2000; Marett, Biros, & Knode, 2004). Research has shown recipients of deceptive messages typically have a poor track record, with accuracy rates most often indistinguishable from random chance (Bond, Jr. & DePaulo, 2006; Miller & Stiff, 1993). When a message lacks veracity, it facilitates deception detection (Gartner, 2010). We predict that when a recipient perceives deception in a message, their intention to comply will be reduced. We therefore posit:

- H6**:** Perceived deception negatively influences behavioral intention to download anti-virus software.

Method

In order to evaluate the factors that impact individual users' perceptions of deception, as well as their intention to obey the deceptive message's instructions, we established a scenario-based experimental research design in which we exposed our subjects to a message that was reflective of a deceptive scareware message. Scenario-based research designs have been recommended as an appropriate method for investigating security behaviors, specifically ones involving deception (Crossler et al., 2013). Subjects of the study followed an email link to an online experiment in which they responded to items about their perceptions of a given scenario. The scenario is a research manipulation that represents a deception, without actually deceiving our subjects. Although we did not actually deceive our subjects (and therefore, did not require ethics board approval of a deceptive research design), we provided our study subjects with a message that would generally be seen as deceptive by a technologically savvy user. In essence, we measured the subjects' perceptions about the deceptiveness of the scareware message and their intention to comply with the instructions in the scareware message.

Whereas phishing normally involves presenting a hyperlink to the intended victim, "Fake Anti-virus" deception usually relies on a set of alternate perceptual stimuli. For the purposes of providing a level of realism and establishing an appropriate usage context, our scenario incorporated the perceptual stimuli normally associated with "Fake Anti-virus." Each research subject was presented with a graphic interface window containing an alert message ending with an exclamation mark in the window's title box. The window also contained a standard warning icon consisting of a red circle, containing a white X. Similar to the Microsoft Windows platform's built-in security software, none of the words in the window are misspelled or in all capital letters, enhancing the user's perception of realism. Also, like standard Microsoft Windows security alert windows, no phishing-like text box was presented, seeking data inputs from the research subject. Instead, the research subject's actions are limited to clicking just one of three buttons: (1) OK, (2) Cancel, or (3) the standard window-closing button at upper right. An additional touch of realism is the use of a standard Microsoft Windows security technique; finishing the message with (Recommended), as is frequently seen with routine system updates. Even security-conscious users would likely find the window presented to be realistic, except that Microsoft Windows does not forbid access to websites pending the download of some particular software.

There was a possibility that research subjects might have believed they had no need of newer anti-virus software, as recommended by the scenario's message window, given that most computers are protected by anti-virus software. However, stories of computer viruses infecting machines in spite of previously installed security software are quite common (Virvilis, Gritzalis, & Apostolopoulos, 2013), potentially leaving the subject in doubt when confronted with an apparent, threat-triggered

recommendation to install anti-virus software. Additionally, frequent, visible updates of built-in software such as Microsoft Windows, installed anti-virus packages, and Adobe Acrobat have accustomed computer users to the concept of an ongoing race between software providers and bad actors. In this context, a research subject might doubt that their computer is protected from every possible virus, as new ones appear every hour of every day. An offer of help to remove a virus that reached the research subject's computer (before it could obtain the most recent update that should have prevented this from occurring in the first place) would certainly appeal to many computer users.

Data sample

With the prevalence of the Internet, almost anyone is subject to the threat of scareware messages that seek to entice the user into purchasing and downloading false security software. However, employees in centralized, tightly controlled networks, are less likely to be exposed to such threats than home users (Warkentin & Johnston, 2006b, 2008). For this reason, subjects drawn from the faculty and staff of a large comprehensive university were selected as an appropriate sample for studying the phenomenon of interest. This sample includes individuals who are "typically already knowledgeable in using computers and the Internet and thus had relatively well-formed perceptions about the capabilities of the web" (Choudhury & Karahanna, 2008). Therefore, this environment and sampling frame reflected the target population—experienced computer users with discretionary control of actions in response to electronic communications particularly over the Internet.

Measures and instrumentation

We measured five constructs: *technology awareness* (TA), *perceived source trustworthiness* (PST), *deception detection self-efficacy* (DDSE), *perceived deception* (PD), and *behavioral intention* (BINT). All of our measurements were multi-item scales adapted from previous research (see Appendix B) with the exception of PD, which was developed for this study but contains items used for measuring deception detection in other contexts (Grazioli & Jarvenpaa, 2000). The general-purpose (GP) questions used in the pre-scenario were adapted from Johnston and Warkentin (2010b). For our measurement of PST, we adapted 7-point semantic differential scales from Berlo, Lemert, and Mertz (1969) with extremes on both sides of the scale. For our measurement of TA, DDSE, and BINT we adapted previously validated multi-item scales based on fully anchored 5-point Likert scales. Technology awareness and deception detection self-efficacy were adapted from Dinev and Hu (2007), who based their items on theories from Bandura (1977), Compeau and Higgins (1995), and Marakas et al. (1998). Behavioral intention was adapted from Venkatesh, Morris, Davis, and Davis (2003). In order to measure perceived deception, we created four items, conducted two expert panel reviews, and implemented feedback from these reviews. Likewise, the measurement of PD used the same fully anchored 5-point Likert scale as our other constructs.

Experimental design and procedure

We conducted this online field experiment among faculty and staff with a total of 331 total of participants who began the experiment; 240 of whom completed the online survey portion of the experiment. The online experiment and survey was created using the Qualtrics platform and utilized a design in which each subject was presented with a screenshot portraying a different randomized scenario. There were 19 responses that did not pass the prequalifying questions (GP) pertaining to their potential exposure to important data, threats, and security. After analyzing the raw data, we removed eight responses where response set was detected (Andrich, 1978; Kerlinger, 1973; Rennie,

1982), leaving us with 213 usable responses. "Response set" is the tendency among subjects to respond to questions randomly, automatically, mindlessly, and/or without regard to reading the content of the items (Andrich, 1978; Kerlinger, 1973). From the usable responses, 65% were male and 35% were female. A quarter of the subjects were between the ages 30 to 39 years, 29% were between 40 and 49, 38% were 50 years and older, and the remaining 8% were younger than 30 years.

After conducting the research design, one item in each of the TA, DDSE, and BINT scales did not load with the other items. In order to further analyze the data, we dropped these items and performed analysis with the remaining items.

Experimental treatment

The experimental procedure for our study involved a pre-scenario instrument, a presentation of a scenario, and a post-scenario instrument as depicted in Figure 3. Due to the nature of the instrument, it was imperative that the subjects be exposed to the items in a prescribed order to avoid introducing bias. Our online procedure did not enable the return to previous measures to ensure that this proper ordering of manipulation and data capture was maintained. Specifically, we measured unmanipulated factors before the scenario manipulation (such as technology awareness) and measured other manipulated factors afterwards, starting with the key DV (intention). By analyzing the actual items in Appendix A, one can see that subjects reading some of the later questions (i.e. deception detection self-efficacy) would have been "tipped off" that the study was about deception, and would have altered their mindset and resulting perceptions, if we did not follow a careful order. It was also critical to measure behavioral intention immediately after the subject read the scenario's scareware message, before any other questions introduced new perspectives in the subject's mind.

The pre-scenario instrument consisted of three general-purpose items and five technology awareness items. The general-purpose questions were used to filter participants for this study. After the pre-scenario survey, subjects were presented with a scenario in which he or she is presented a scareware message while visiting a familiar or unfamiliar website. Consistent with actual scareware, the message manipulation imitated an antivirus program and recommended the subject download the software prior to browsing the rest of the website. Figure 4 provides an example of the message, which was presented as a screenshot in the instrument which required no actual interaction. Subsequent responses were based on individual perceptions of the message manipulation. Immediately following the stimulus, the post-scenario instrument presented the subjects with three items to measure behavioral intention, the primary dependent variable in our model. Then the subject responded to four perceived source trustworthiness items, three deception detection self-efficacy items, and four perceived deception items. These items evaluated whether the subject perceived the message to be deceptive and whether he or she intended to interact with this scareware message. Finally, basic demographic information was collected. See Appendix A for the full instrument.

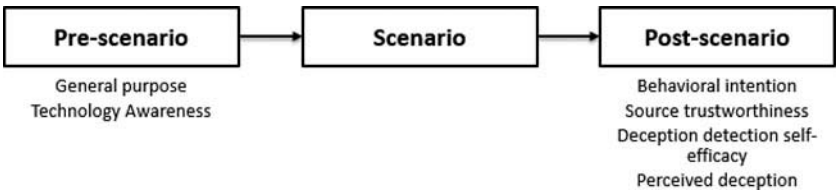

Figure 3. Experimental procedure.

Figure 4. Warning message for downloading the scareware.

Data analysis and results

Instrument validity

Data analysis was conducted using SmartPLS 3.0. SmartPLS is considered to be effective for analyses incrementing established relationships (i.e., source credibility and behavioral intention) with new constructs (i.e., perceived deception) and structural paths. It is useful in validating models using component-based structural equation modeling and is more appropriate than covariance-based techniques (Chin, Marcolin, & Newsted, 2003; Gefen & Straub, 2005; Reinartz, Haenlein, & Henseler, 2009). We generated a bootstrap with 500 resamples to test our model. In addition, we assessed model fit and reliability.

The fit indices suggest that our model was a good fit to the data (see Table 2). To establish good fit, χ^2 (chi-square) was measured and the χ^2 index (χ^2/df = 387.3/499) was computed. The χ^2 index is better measurement of fit than χ^2 because it is less sensitive to sample size. The χ^2 index should be at a maximum 5 (Schumacker & Lomax, 2004) and below 3 for acceptable fit (Kline, 1998). Additionally, the standard root mean square residual (SRMR) statistic which is often used to avoid misspecification (Henseler et al., 2014) indicates good fit where anything less than 0.10 (or less than 0.08 in the more conservative version) is considered to have good fit (Hu & Bentler, 1999). Additionally, all

Table 2. Confirmatory factor analysis.

	Standardized Factor Loadings
Technology Awareness (ρ = 0.85)	
I follow news and developments about computer viruses	0.743
I discuss Internet security issues with friends and others	0.776
I have read about malicious software intruding users' computers.	0.794
I am aware of virus problems and consequences.	0.766
Perceived Source Trustworthiness (ρ = 0.96)	
Untrustworthy—Trustworthy	0.933
Dangerous—Safe	0.960
Disreputable—Reputable	0.932
Unreliable—Reliable	0.897
Deception Detection Self-efficacy (ρ = 0.95)	
I am confident I can detect deception in electronic communications.	0.944
I am able to detect deception in electronic communication without much effort.	0.949
Perceived Deception (ρ = 0.96)	
I believe the virus message was not truthful.	0.843
I believe the message in the scenario was designed to trick me.	0.955
The virus message was not legitimate.	0.945
The intent of the virus message was to deceive me.	0.963
Behavioral Intention (ρ = 0.86)	
I predict I would use the recommended anti-virus software.	0.894
In this situation, I would plan to use the anti-virus software.	0.833
Model Fit Statistics:	
χ^2 = 387.30, df = 499; SRMR = 0.058	

Note: ρ = composite reliability; SRMR = Standardized Root Mean Square Residual.

Table 3. Means, standard deviations, and correlations of constructs.

				Intercorrelations of Constructs				
Construct	Mean	SD	AVE	1	2	3	4	5
1. TA	3.75	0.70	0.593	**0.770**				
2. PST	1.49	1.00	0.866	−0.203	**0.931**			
3. DDSE	2.92	1.01	0.895	0.310	−0.228	**0.946**		
4. PD	4.54	0.78	0.860	0.139	−0.364	0.257	**0.928**	
5. BI	1.46	0.81	0.747	−0.125	0.317	−0.214	−0.210	**0.864**

Note: SD. = standard deviation; AVE = average variance extracted; values on the diagonal are the square root of AVE for each construct.

constructs had an acceptable level (≥ 0.70, see Table 2) of reliability (Mackenzie, Podsakoff, & Podsakoff, 2011; Peter, 1979). Initial reliability scores were obtained through reliability analysis by computing composite reliability.

Convergent and discriminant validity of the measures were then assessed. Convergent validity, as defined by Campbell and Fiske (Campbell & Fiske, 1959), is established when items of the same construct correlate at a significant level with each other. As indicated in Tables 2 and 3, all of our constructs displayed convergent validity as they had item loadings greater than 0.70 (with no cross-loadings) and average variance explained (AVE) above 0.50 (Gefen & Straub, 2005).

All constructs displayed discriminant validity; item-to-construct correlations are higher with each other than with other construct measures and their composite values (Loch, Straub, & Kamel, 2003). Discriminant validity is confirmed by comparing the square root of AVE statistics against correlation measures of other constructs (Gefen, Straub, & Boudreau, 2000). The square root of AVE was greater than inter-construct correlations and item loadings were greater than the loadings on other constructs (see Table 3).

Common method bias

Systematic bias occurs when both the predictor and outcome variables are collected at a single point in time rather than longitudinally. This bias, also known as common method variance (CMV), can be addressed both procedurally and statistically (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003); however, procedural (proactive) remedies are more important (Burton-Jones, 2009; Richardson, Simmering, & Sturman, 2009). During scale development and evaluation procedures, it is necessary to examine common method effects that are possible due to source or rater, item characteristics, item context, and measurement context (Podsakoff et al., 2003). Scenarios and scales developed for this study underwent extensive expert panel reviews as suggested in previous research (Petter, Straub, & Rai, 2007; D. W. Straub, Boudreau, & Gefen, 2004) to address these sources of common method effects and ensure realism, content validity, and face validity.

Path model analysis results

After establishing instrument validity, we tested our path model using the bootstrap method to determine the significance of our path estimates between constructs. The model fits the data well (see Table 4). The χ^2 index and SRMR fit statistics were within recommended levels. We then obtained the standardized path estimate for each hypothesis in the model (see Table 4 and Figure 5) and all paths were found statistically significant explaining 16.5% of the variance of perceived deception and 7.2% of the variance of behavioral intention.

Table 4. Structural model test results for customers.

Hypothesized Relationship	Standardized Estimate	T Value	p Value	Hypothesis Supported
H1: TA → PST (-)	−0.203	3.168	0.0016	Yes
H2: TA → DDSE (+)	0.310	5.038	0.0000	Yes
H3: PST → PD (-)	−0.322	3.603	0.0003	Yes
H4: DDSE → PD (+)	0.184	2.613	0.0093	Yes
H5: DDSE → BINT (-)	−0.172	2.665	0.0079	Yes
H6: PD → BINT (-)	−0.166	1.994	0.0467	Yes
Squared Multiple Correlations				
PST	0.041			
DDSE	0.096			
PD	0.165			
BINT	0.072			
Model Fit Statistics	χ^2 = 387.30, df = 499; SRMR = 0.058			

Note: SRMR = Standardized root mean square residual

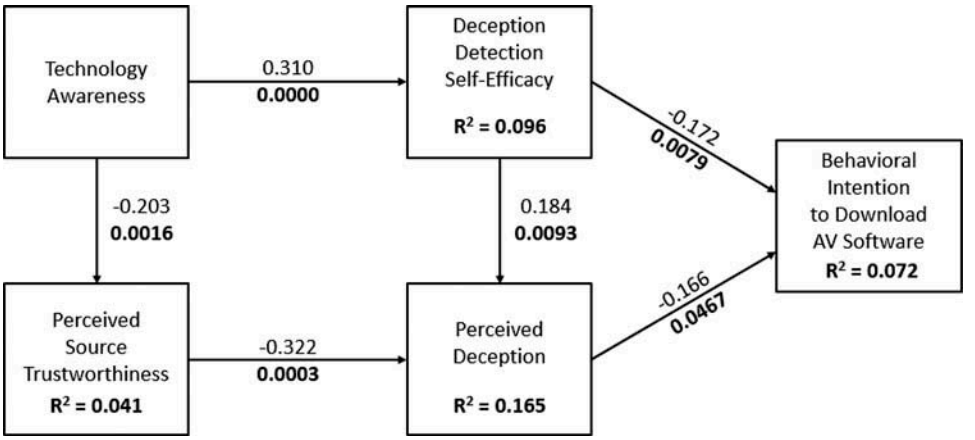

Figure 5. Warning message for downloading the scareware.

Discussion and contribution

What factors impact an Internet user's ability to perceive deception and reject computer security threats? What enhances these factors and indirectly reduces the likelihood of succumbing to deception? The findings of this study provide answers to these questions and also highlight several factors for protecting against malicious software which can inform practitioners seeking to support their users' ability to detect and respond appropriately to acts of deception. Further, the results of this study advance the literature focused on this phenomenon and our understanding of how best to model the dynamic interactions among factors that influence deception detection in Internet users.

In essence, users who are more aware of security issues will be more cautious and discerning of the source of a message and perceive themselves as more adept at detecting deception in the messages. These findings indicate support for hypotheses 1 and 2, but perhaps more importantly accentuate the need for organizations to train users against possible security threats, even from sources that are generally deemed trustworthy. Recent research reveals that training activities focused on the appropriate use of technology should accentuate historical and social processes, focused on authentic problems and tasks (Hung, 2001; Puhakainen & Siponen, 2010). This underscores the need for user training that presents actual deception, perhaps utilizing actual scareware messages captured by IS management personnel. These training efforts should also encourage discussion and interaction among users, thereby delivering the potential of social processes as a formidable component of an effective training program. A wiki site dedicated to scareware incidents

that have occurred within the organization may be an optimal tool for continued awareness training through historical and social processes. Such training may lead to higher levels of deception detection self-efficacy which would raise awareness of possible security threats and would protect organizational systems because employees would be less susceptible to scareware.

As the findings of this study indicate, perceptions of deception are directly influenced by one's confidence in the ability to detect deception as well as perceptions about the trustworthiness of the message source. Beyond indicating support for hypotheses 3 and 4, these findings point to the need for transparency in security-related communication as well as the development of efficacy among users, as previously suggested. Transparency in communication, while somewhat challenging for organizations dependent upon external security monitoring services, is more readily accomplished in organizations that are aware of the value of open communication models and have a structured organizational communication hierarchy where security messages are championed by trusted executives and peer leaders. This finding further supports previous research which has demonstrated that source trustworthiness is an important factor in the effectiveness of a security message (Johnston & Warkentin, 2010b), but extends this insight by attributing source trustworthiness to one's perceptions of deception originating from message exposure, a previously unexplored relationship.

Finally, the results indicate support for hypotheses 5 and 6; individuals with a high degree of deception detection self-efficacy and those who perceive the scareware message to be deceptive are not likely to form the intention to follow its recommendation and download the software. Of course, if deception is detected, it should be expected that users will reject any recommendations provided within the message. But, interestingly, the results suggest that deception detection self-efficacy also increases the likelihood for forming intentions to comply with the message recommendations. By encouraging users to be more skeptical with messages they receive on their computer or while browsing the Internet, users may more effectively identify deceptive messages, decreasing the possibility of personal or organizational information being stolen or of systems being infected.

Limitations and future research

The present study identifies factors that enable users to perceive deception and to take the necessary actions to reject these deceptive messages. The use of university faculty and staff as research subjects may be a limitation of our research design. In a university setting, addressing relevant threats may not be a high priority or social norm (Johnston & Warkentin, 2010a); hence, results may not be generalizable to some industry settings. Additionally, university faculty and staff on average have much higher levels of educational attainment than the general population, which may have affected the results. However, 92% of the research participants were 30 years of age or older, making them fairly representative of the overall adult population.

Another limitation is the construct of perceived deception instead of deception detection. Our instrument was only able to measure an individual's perceptions of deception. This approach is due to fact that we did not actually deceive the respondents; instead, we invoked them to judge the validity of a message. Given that individuals who are warned beforehand have the most realistic chance of uncovering lies (George, Marett, & Tilley, 2004), the perception of deception may be just as important as actual detection. Encouraging users to be more skeptical may be more favorable in influencing these perceptions resulting in less susceptibility to deceitful and often malicious messages.

Actual behavior was not measured in our research; rather, we measured behavioral intention. However, the role of intention as a predictor of behavior has been well established in IS research (Ajzen, 1991; Sheppard, Hartwick, & Warshaw, 1988; Taylor & Todd, 1995). Nevertheless, actual behavior can sometimes be different than behavioral intention as intention is normally self-reported.

In a future study, source familiarity could be re-examined to determine its impact on other factors in our model, perhaps in a replication of our study. (Our manipulation of this factor failed to yield any interesting findings to report.) *Familiarity* is knowing or understanding a company or source,

who it is, and what it stands for (Pavlou, Tan, & Gefen, 2003). Through repeated communicative transactions with a familiar partner, a baseline model of normal exchanges would be established which would enable an individual to identify an unusual, suspicious message. Individuals are believed to reach an appropriate level of suspicion based on comparisons with a baseline model (Carlson & George, 2004). As a result, we expect familiarity will influence the degree to which an individual finds a message to be deceptive or not.

A related area for future exploration is the differentiation between perceptions of the original source of the message and the media for conveyance. For example, if a pop-up message about security appears while visiting a website, will the user perceive the credibility of the local security application or the website being visited? Or will the browser itself be seen as the source? Lee, Warkentin, and Johnston (2016) evaluate this "chain" of communications media encountered when engaging on online transactions and inform researchers about the risk factors one might encounter. This nuanced investigation of the source credibility component could be further explored in future deception detection studies.

Additionally, future research could focus on the role of training with regard to identifying deceptive messages. Researchers could perform a longitudinal study where factors that influence perceived deception would initially be measured. The research participants would then be trained to identify scareware, and researchers could later evaluate whether individuals were susceptible to other deceptive messages in an online context.

Conclusions

Vigilance among users has often been cited as a critical element in securing individual and organizational assets from malicious software and attacks. Historically, this understanding has been applied toward traditional malware forms, such as those that surreptitiously embed viruses or spyware within unprotected systems and software applications. With the emergence of scareware and related warning-based social engineering attacks, users are faced with another form of deception.

In this paper, we introduced the role that perceived deception plays in influencing behavioral intention in a scareware context, and we studied the factors that influence perceived deception. Our results indicate that deception detection self-efficacy had a significant impact on whether individuals perceived a scareware message to be deceptive and whether individuals had intentions to act on the recommendations of the scareware message. Source trustworthiness was also identified as a significant factor that influenced perceptions of deception. Additionally, technology awareness was shown to increase perceptions of source trustworthiness and deception detection self-efficacy. Finally, messages viewed as deceptive are more likely to be rejected, reducing individual intent to download potentially harmful software. These findings underscore the need for training to increase technology awareness and deception detection self-efficacy.

ORCID

Dustin Ormond http://orcid.org/0000-0003-0009-6594
Merrill Warkentin http://orcid.org/0000-0001-7435-7676
Allen C. Johnston http://orcid.org/0000-0003-0301-4187
Samuel C. Thompson http://orcid.org/0000-0003-4856-9100

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*, 179–211. doi:10.1016/0749-5978(91)90020-T

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

Allen, D. G., Mahto, R. V., & Otondo, R. F. (2007). Web-based recruitment: Effects of information, organizational brand, and attitudes toward a Web site on applicant attraction. *The Journal of Applied Psychology*, *92*(6), 1696–1708. doi:10.1037/0021-9010.92.6.1696

Alowibdi, J. S., Buy, U. A., Yu, P. S., Ghani, S., & Mokbel, M. (2015). Deception detection in Twitter. *Social Network Analysis and Mining*, *5*(1), 1–16. doi:10.1007/s13278-015-0273-1

Andrich, D. (1978). A rating formulation for ordered response categories. *Psychometrika*, *43*(4), 561–573. doi:10.1007/BF02293814

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191–215. doi:10.1037/0033-295X.84.2.191

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist*, *37*(2), 122–147. doi:10.1037/0003-066X.37.2.122

Bandura, A. (1995). *Self-efficacy in changing societies*. Cambridge, UK: Cambridge University Press.

Berlo, D. K., & Lemert, J. B. (1961). A factor analytic study of the dimensions of source credibility. In 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. doi:10.1086/267745

Bond, Jr., C. F., & DePaulo, B. M. (2006). Accuracy of deception judgments. *Personality and Social Psychology Review*, *10*(3), 214–234. doi:10.1207/pspr.2006.10.issue-3

Buller, D. B., & Burgoon, J. K. (1996). Interpersonal deception theory. *Communication Theory*, *6*(3), 203–242. doi:10.1111/comt.1996.6.issue-3

Burgoon, J. K., Buller, D. B., Ebesu, A. S., & Rockwell, P. (1994). Interpersonal deception: V. accuracy in deception detection. *Communication Monographs*, *61*(4), 303–325. doi:10.1080/03637759409376340

Burton-Jones, A. (2009). Minimizing method bias through programmatic research. *MIS Quarterly*, *33*(3), 445–471.

Butler, C. (2016). *How scary is the new Mac scareware?* Retrieved January 1, 2016, from https://computerbutler.net/2016/02/scary-new-mac-scareware/

Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin*, *56*(2), 81–105. doi:10.1037/h0046016

Carlson, J. R., & George, J. F. (2004). Media appropriateness in the conduct and discovery of deceptive communication: The relative influence of richness and synchronicity. *Group Decision and Negotiation*, *13*, 191–210. doi:10.1023/B:GRUP.0000021841.01346.35

Carlson, J. R., & Zmud, R. W. (1999). Channel expansion theory and the experiential nature of media richness perceptions. *Academy of Management Journal*, *42*(2), 153–170. doi:10.2307/257090

Caspi, A., & Gorsky, P. (2006). Online deception: Prevalence, motivation, and emotion. *CyberPsychology & Behavior*, *9*(1), 54–59. doi:10.1089/cpb.2006.9.54

Chen, J. Q., Schmidt, M. B., Phan, D. D., & Arnett, K. P. (2008). E-commerce security threats: Awareness, trust and practice. *International Journal of Information Systems and Change Management*, *3*(1), 16–32. doi:10.1504/IJISCM.2008.019287

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research*, *14*(2), 189–217. doi:10.1287/isre.14.2.189.16018

Choudhury, V., & Karahanna, E. (2008). The relative advantage of electronic channels: A multidimensional view. *MIS Quarterly*, *32*(1), 179–200.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, *19*(2), 189–211. doi:10.2307/249688

Constantin, L. (2015). *Scareware found hidden in Google Play apps downloaded by millions*. Retrieved January 1, 2016, from http://www.pcworld.com/article/2879952/scareware-found-hidden-in-google-play-apps-downloaded-by-millions.html

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*(1), 90–101. doi:10.1016/j.cose.2012.09.010

DePaulo, B. M., Charlton, K., Cooper, H., Lindsay, J. J., & Muhlenbruck, L. (1997). The accuracy-confidence correlation in the detection of deception. *Personality and Social Psychology Review*, *1*(4), 346–357. doi:10.1207/pspr.1997.1.issue-4

Dhamija, R. R., Tygar, J. D., & Hearst, M. M. (2006). Why phishing works. In SIGCHI Conference on Human Factors in Computing Systems (pp. 1581–1590). Montreal, Quebec, Canada.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, *8*(7), 386–408.

Ebot, A. C. T., & Siponen, M. (2014). Toward a rational choice process theory of Internet scamming: The offender's perspective. In International Conference on Information Systems. New Zealand.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior*. Reading, MA: Addison-Wesley.

Fuller, C. M., Marett, K., & Twitchell, D. P. (2012). An examination of deception in virtual teams: Effects of deception on task performance, mutuality, and trust. *IEEE Transactions on Professional Communication*, *55*(1), 20–35. doi:10.1109/TPC.2011.2172731

Gartner. (2010). *Gartner highlights key predictions for IT organizations and users in 2010 and beyond*. Retrieved from http://www.gartner.com/it/page.jsp?id=1278413

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*(5), 91–109.
Gefen, D., Straub, D. W., & Boudreau, M.-C. (2000). Structural equation modeling techniques and regression: Guidelines for research practice. *Communications of the Association for Information Systems*, *4*(7), 1–77.
George, J. F., Marett, K., & Tilley, P. (2004). Deception detection under varying electronic media and warning conditions. In Proceedings of the 37th Hawaii International Conference on System Sciences (Vol. 00, pp. 1–9).
George, J. F., & Robb, A. (2008). Deception and computer-mediated communication in daily life. *Communication Reports*, *21*(2), 92–103. doi:10.1080/08934210802298108
Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users: A study of perceptions of the adequacy of security. *Information & Management*, *20*(1), 13–27. doi:10.1016/0378-7206(91)90024-V
Granhag, P. A., & Vrij, A. (2005). Psychology and law: An empirical perspective. In N. Brewer & K. D. Williams (Eds.), *Deception detection* (pp. 43–92). New York, NY: Guilford Press.
Grazioli, S. (2004). Where did they go wrong? An analysis of the failure of knowledgeable Internet consumers to detect deception over the Internet. *Group Decision and Negotiation*, *13*(2), 149–172. doi:10.1023/B:GRUP.0000021839.04093.5d
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. doi:10.1109/3468.852434
Hancock, J. T., Toma, C., & Ellison, N. (2007). The truth about lying in online dating profile. In Proceedings of the SIGCHI 2007 Conference on Human Factor in Computing Systems (pp. 449–452). San Jose, CA.
Hancock, J. T., Woodworth, M. T., & Goorha, S. (2010). See no evil: The effect of communication medium and motivation on deception detection. *Group Decision and Negotiation*, *19*(4), 327–343. doi:10.1007/s10726-009-9169-7
Henseler, J., Dijkstra, T. K., Sarstedt, M., Ringle, C. M., Diamantopoulos, A., Straub, D. W. … Calantone, R. J. (2014). Common beliefs and reality about PLS: Comments on Ronkko and Evermann (2013). *Organizational Research Methods*, *17*(2), 182–209. doi:10.1177/1094428114526928
Ho, S. M., Lowry, P. B., Warkentin, M., Yang, Y., & Hollister, J. M. (2016). Gender deception in asynchronous online communication: A path analysis. *Information Processing & Management*. doi:10.1016/j.ipm.2016.06.004
Ho, S. M., & Warkentin, M. (2015). Leader's dilemma game: An experimental design for cyber insider threat research. *Information Systems Frontiers*, 1–20. doi:10.1007/s10796-015-9599-5
Hovland, C. I., Janis, I. L., & Kelley, H. H. (1953). *Communication and persuasion*. New Haven, CT: Yale University Press.
Hovland, C. I., & Weiss, W. (1951). The influence of source credibility on communication effectiveness. *Public Opinion Quarterly*, *15*(4), 635–650. doi:10.1086/266350
Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, *6*(1), 1–55. doi:10.1080/10705519909540118
Hung, D. (2001). Theories of learning and computer-mediated instructional technologies. *Educational Media International*, *38*(4), 281–287. doi:10.1080/09523980110105114
Jensen, M. L., Lowry, P. B., Burgoon, J. K., & Nunamaker, J. F. (2010). Technology dominance in complex decision making: The case of aided credibility assessment. *Journal of Management Information Systems*, *27*(1), 175–202. doi:10.2753/MIS0742-1222270108
Jensen, M. L., Lowry, P. B., & Jenkins, J. L. (2011). Effects of automated and participative decision support in computer-aided credibility assessment. *Journal of Management Information Systems*, *28*(1), 201–234. doi:10.2753/MIS0742-1222280107
Johnston, A. C., & Warkentin, M. (2010a). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549–566.
Johnston, A. C., & Warkentin, M. (2010b). The influence of perceived source credibility on end user attitudes and intentions to comply with recommended IT actions. *Journal of Organizational and End User Computing*, *22*(3), 1–21. doi:10.4018/JOEUC
Joinson, A. N., & Dietz-Uhler, B. (2002). Explanations for the perpetration of and reactions to deception in a virtual community. *Social Science Computer Review*, *20*(3), 275–289. doi:10.1177/08939302020003005
Jones, H. S., Towse, J. N., & Race, N. (2015). Susceptibility to email fraud: A review of psychological perspectives, data-collection methods, and ethical considerations. *International Journal of Cyber Behavior, Psychology and Learning*, *5*(3), 13–29. doi:10.4018/IJCBPL
Kaplan, A. M., & Haenlein, M. (2011). Two hearts in three-quarter time: How to waltz the social media/viral marketing dance. *Business Horizons*, *54*(3), 253–263. doi:10.1016/j.bushor.2011.01.006
Kelman, H. C., & Hovland, C. I. (1953). Reinstatement of the communicator in delayed measurement of opinion change. *The Journal of Abnormal and Social Psychology*, *48*(3), 327–335. doi:10.1037/h0061861
Kerlinger, F. N. (1973). *Foundations of behavioral research* (2nd ed.). London, UK: Holt Reinhart & Winston.
Kline, R. B. (1998). *Principles and practice of structural equation modeling*. New York, NY: Guilford Press.

Larsen, C. (2011). *Busting a big malvertising/fake-AV attack*. Retrieved from https://www.bluecoat.com/security/security-archive/2011-07-25/busting-big-malvertising-fake-av-attack-0

Larsen, C. (2013). *Blocking a fake "browser update" site*. Blue Cost Systems, Inc. Retrieved from https://www.bluecoat.com/security-blog/2013-10-14/blocking-fake-browser-update-site

Lee, J., Jr., Warkentin, M., & Johnston, A. C. (2016). A broader view of perceived risk during internet transactions. *Communications of AIS*, *38*(8), 171–189.

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. doi:10.1109/TEM.2002.808257

Mackenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly*, *35*(2), 293–334.

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. doi:10.1287/isre.9.2.126

Marett, K., Biros, D. P., & Knode, M. L. (2004). Self-efficacy, training effectiveness, and deception detection: A longitudinal study of lie detection training. *Intelligence and Security Informatics*, *3073*, 187–200.

Marett, K., & George, J. F. (2004). Deception in the case of one sender and multiple receivers. *Group Decision and Negotiation*, *13*(1), 29–44. doi:10.1023/B:GRUP.0000011943.73672.9b

Martinez-Cabrera, A., & Kim, R. (2010). *Google warns of fake anti-virus programs popping up online*. Retrieved from http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2010/04/16/BUI71CVV5P.DTL

Miller, G., & Stiff, J. B. (1993). *Deceptive communication*. Newbury Park, CA: Sage Publications, Inc.

Mills, E. (2010). *Ads to blame for malware in Facebook's farm town?* Retrieved from http://www.cnet.com/news/ads-to-blame-for-malware-in-facebooks-farm-town/#!

Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology*, *25*(2), 243–262. doi:10.1016/S0167-4870(02)00172-1

Pavlou, P., Tan, Y.-H., & Gefen, D. (2003). Institutional trust and familiarity in online interorganizational relationships. In Proceedings of the 36th Annual Hawaii International Conference on System Sciences (Vol. 16, pp. 215–224). Big Island, Hawaii.

Pennington, R., Wilcox, H. D., & Grover, V. (2004). The role of system trust in business-consumer transactions. *Journal of Management Information Systems*, *20*(3), 197–226.

Peter, J. P. (1979). Reliability: A review of psychometric basics and recent marketing practices. *Journal of Marketing Research*, *16*(1), 6–17. doi:10.2307/3150868

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

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879–903. doi:10.1037/0021-9010.88.5.879

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, *34*(4), 757–778.

Reinartz, W., Haenlein, M., & Henseler, J. (2009). An empirical comparison of the efficacy of covariance-based and variance-based SEM. *International Journal of Research in Marketing*, *26*(4), 332–344. doi:10.1016/j.ijresmar.2009.08.001

Rennie, L. J. (1982). Detecting a response set to Likert-style attitude items with the rating model. *Education Research and Perspectives*, *9*(1), 114–118.

Richardson, H. A., Simmering, M. J., & Sturman, M. C. (2009). A tale of three perspectives: Examining post hoc statistical techniques for detection and correction of common method variance. *Organizational Research Methods*, *12*(4), 762–800. doi:10.1177/1094428109332834

Schumacker, R. E., & Lomax, R. G. (2004). *A beginner's guide to structural equation modeling* (2nd ed.). Mahwah, NJ: Lawrence Erlbaum.

Sheppard, B. H., Hartwick, J., & Warshaw, P. R. (1988). The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research. *Journal of Consumer Research*, *15*(3), 325–343. doi:10.1086/jcr.1988.15.issue-3

Sophos. (2010). *What is FakeAV?* Retrieved from http://sophos.williams.edu/media/what-is-fakeav.pdf

Sophos. (2011a). *Security threat report 2011*. Security. Retrieved from http://www.sophos.com/medialibrary/GatedAssets/white papers/sophossecuritythreatreport2011wpna.pdf

Sophos. (2011b). *Stopping fake antivirus: How to keep scareware off your network*. A Sophos White Paper. Retrieved from http://resources.idgenterprise.com/original/AST-0052862_sophos-stopping-fake-antivirus-wpna-sept11.pdf

Stone-Gross, B., Abman, R., Kemmerer, R. A., Kruegel, C., Steigerwald, D. G., & Vigna, G. (2011). *The underground economy of fake antivirus software*. Santa Barbara, CA: University of California, Santa Barbara.

Straub, D. W., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, *13*(1), 381–427.

Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research*, *6*(2), 144–176. doi:10.1287/isre.6.2.144

Twyman, N. W., Lowry, P. B., Burgoon, J. K., & Nunamaker, J. F. (2014). Autonomous scientifically controlled screening systems for detecting information purposely concealed by individuals. *Journal of Management Information Systems*, *31*(3), 106–137. doi:10.1080/07421222.2014.995535

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425–478.

Virvilis, N., Gritzalis, D., & Apostolopoulos, T. (2013). Trusted Computing vs. Advanced Persistent Threats. In Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC) (pp. 396–403). Vietri sul Mere, Italy.

Vrij, A. (2001). *Detecting lies and deceit*. Chichester, UK: Wiley.

Wang, W., & Benbasat, I. (2007). Recommendation agents for electronic commerce: Effects of explanation facilities on trusting beliefs. *Journal of Management Information Systems*, *23*(4), 217–246. doi:10.2753/MIS0742-1222230410

Warkentin, M., & Johnston, A. C. (2006a). An XML-based intelligent agent protocol design framework for individualized privacy postures within trusted network environments. *Journal of Information Privacy and Security*, *2*(1), 16–28. doi:10.1080/15536548.2006.10855784

Warkentin, M., & Johnston, A. C. (2006b). IT security governance and centralized security controls. In M. Warkentin, & R. B. Vaughn (Eds.), *Enterprise information systems assurance and system security: Managerial and technical issues* (1st ed., pp. 16–24). Hershey, PA: Idea Group Publishing.

Warkentin, M., & Johnston, A. C. (2008). IT governance and organizational design for security management. In D. Straub, S. Goodman, & R. L. Baskerville (Eds.), *Information security policies and practices* (pp. 46–68). Armonk, NY: M. E. Sharpe.

Wright, R. T., Chakraborty, S., Basoglu, A., & Marett, K. (2009). Where did they go right? Understanding the deception in phishing communications. *Group Decision and Negotiation*, *19*(4), 391–416. doi:10.1007/s10726-009-9167-9

Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, *27*(1), 273–303. doi:10.2753/MIS0742-1222270111

Yoon, S.-J. (2002). The antecedents and consequences of trust in online-purchase decisions. *Journal of Interactive Marketing*, *16*(2), 47–63. doi:10.1002/dir.10008

Zhou, L., Burgoon, J. K., Twitchell, D. P., Qin, T., & Nunamaker, J. F. (2004). A comparison of classification methods for predicting deception in computer-mediated communication. *Journal of Management Information Systems*, *20*(4), 139–165.

Zorz, Z. (2016). *Mac users beware! Scareware hides behind fake Flash Player update*. Retrieved January 1, 2016, from https://www.helpnetsecurity.com/2016/02/05/mac-users-beware-scareware-hides-behind-fake-flash-player-update/

Appendix A: Instrument

Please indicate the degree to which you agree with each statement (1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, and 5 = Strongly Agree).

Section 1

General Purpose (Filter Questions)	1	2	3	4	5
1. I maintain important data on a specific computer (GP1).					
2. I am responsible for the detection and prevention of threats to the data on that computer (GP2).					
3. I am concerned for the security of the data on that computer (GP3).					

Section 2

Technology Awareness (TA)	1	2	3	4	5
4. I follow news and developments about computer viruses (TA1).					
5. I discuss Internet security issues with friends and others (TA2).					
6. I have read about malicious software intruding users' computers (TA3).					
7. I seek advice about anti-virus software (TA4).					
8. I am aware of virus problems and consequences (TA5).					

Section 3: Scenario Treatment

While surfing the web to casually read about an interest of yours, you see a link to a [familiar/unfamiliar] website you have [used many times/never visited before]. When you click on it, the following message appears …

Please indicate the degree to which you agree with each statement (1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, and 5 = Strongly Agree).

Section 4

Behavioral Intention (BINT)	1	2	3	4	5
9. In this scenario, I would download the anti-virus software (BINT1).					
10. I predict I would use the recommended anti-virus software (BINT2).					
11. In this situation, I would plan to use the anti-virus software (BINT3).					

Section 5: Source Credibility

Please check the appropriate box the term that best captures your beliefs about the message source.

	Neutral	
12. Untrustworthy (PST1)		Trustworthy
13. Dangerous (PST2)		Safe
14. Disreputable (PST3)		Reputable
15. Unreliable (PST4)		Reliable

Please indicate the degree to which you agree with each statement (1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, and 5 = Strongly Agree).

Section 6

Deception Detection Self-Efficacy (DDSE)	1	2	3	4	5
16. Detecting deception in electronic communication is easy to do (DDSE1).					
17. I am confident I can detect deception in electronic communications (DDSE2).					
18. I am able to detect deception in electronic communication without much effort (DDSE3).					

Section 7

Perceived Deception (PD)	1	2	3	4	5
19. I believe the virus message was not truthful (PD1).					
20. I believe the message in the scenario was designed to trick me (PD2).					
21. The virus message was not legitimate (PD3).					
22. The intent of the virus message was to deceive me (PD4).					

Section 8: Demographic Information

The demographic information in this section will only be used in aggregate form and will not be used to identify individual respondents. Please select only one item in each category.

Gender	Age	Highest Level of Education
[ ] male	[ ] 18 to 21	[ ] high school
[ ] female	[ ] 22 to 29	[ ] some college
	[ ] 30 to 39	[ ] bachelor's degree
	[ ] 40 to 49	[ ] master's degree
	[ ] 50 and over	[ ] doctorate
		[ ] other

Thank you for participating in this study.

Appendix B: Origination of scale items for research constructs

Construct	Adapted Scale Items	Original Scale Items	Source
Technology Awareness (TA)	I follow news and developments about computer viruses.	I follow news and developments about the spyware technology.	Dinev and Hu (2007)
	I discuss Internet security issues with friends and others.	I discuss with friends and people around me security issues of Internet.	
	I have read about malicious software intruding users' computers.	I read about the problems of malicious software intruding Internet users' computers.	
	I seek advice about anti-virus software.	I seek advice on computer web sites or	
	I am aware of virus problems and consequences.	magazines about anti-spyware products. I am aware of the spyware problems and consequences.	
Perceived Source Trustworthiness (PST)	Untrustworthy—Trustworthy	Untrustworthy—Trustworthy	Berlo et al. (1969)
	Dangerous—Safe	Dangerous—Safe	
	Disreputable—Reputable	Disreputable—Reputable	
	Unreliable—Reliable	Unreliable—Reliable	
Deception Detection Self-efficacy (DDSE)	Detecting deception in electronic communication is easy to do.	I am confident that I can clean spyware off my system	Dinev and Hu (2007)
	I am confident I can detect deception in electronic communications.	I am confident I can prevent unauthorized intrusion to my computer.	
	I am able to detect deception in electronic communication without much effort.	I believe I can configure my computer to provide good protection from spyware.	
Perceived Deception (PD)	I believe the virus message was not truthful.	—	Developed for this study.
	I believe the message in the scenario was designed to trick me.		
	The virus message was not legitimate.		
	The intent of the virus message was to deceive me.		
Behavioral Intention (BINT)	In this scenario, I would download the anti-virus software.	I intend to use the system in the next<n> months.	Venkatesh et al. (2003)
	I predict I would use the recommended anti-virus software.	I predict I would use the system in the next <n> months.	
	In this situation, I would plan to use the anti-virus software.	I plan to use the system in the next <n> months.	