International Journal of Human–Computer Interaction

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/hihc20

Do Warning Message Design Recommendations Address Why Non-experts Do Not Protect Themselves from Cybersecurity Threats? A Review

Keith S. Jones, Natalie R. Lodinger, Benjamin P. Widlus, Akbar Siami Namin & Rattikorn Hewett

To cite this article: Keith S. Jones, Natalie R. Lodinger, Benjamin P. Widlus, Akbar Siami Namin & Rattikorn Hewett (2021): Do Warning Message Design Recommendations Address Why Non-experts Do Not Protect Themselves from Cybersecurity Threats? A Review, International Journal of Human–Computer Interaction, DOI: 10.1080/10447318.2021.1908691

To link to this article: https://doi.org/10.1080/10447318.2021.1908691

INTERNATIONAL JOURNAL OF HUMAN–COMPUTER INTERACTION
https://doi.org/10.1080/10447318.2021.1908691

Taylor & Francis
Taylor & Francis Group

SURVEY ARTICLE

Do Warning Message Design Recommendations Address Why Non-experts Do Not Protect Themselves from Cybersecurity Threats? A Review

Keith S. Jones[a], Natalie R. Lodinger[a], Benjamin P. Widlus[a], Akbar Siami Namin[b], and Rattikorn Hewett[b]

[a]Department of Psychological Sciences, Texas Tech University, Lubbock, Texas, USA; [b]Department of Computer Science, Texas Tech University, Lubbock, Texas, USA

ABSTRACT

We aimed to understand whether warning message design recommendations address the reasons why non-experts choose to *not* protect themselves from cybersecurity threats. Toward that end, we synthesized literature to investigate why non-experts choose to *not* protect themselves, and catalog design recommendations aimed at influencing how non-experts think about threats. We then evaluated whether those recommendations addressed non-experts' reasons. We are the first to synthesize and compare these important literatures. Our results revealed that current recommendations do not adequately address many of non-experts' reasons for *not* protecting themselves. Therefore, implementing those recommendations probably will not convince those non-experts to protect themselves, which may partially explain why warning messages that implement current recommendations improve user compliance but to levels that are still lower than desired. Our results also highlight the need for future research that could lead to new warning message design recommendations that better address non-experts' reasons for *not* protecting themselves.

1. Introduction

Many recommendations regarding how to best warn users about potential cybersecurity threats advocate providing information that will influence how non-experts think about threats (Bartsch et al., 2013; Bravo-Lillo et al., 2011a; Hardee et al., 2006; Ibrahim et al., 2010; Kauer et al., 2012; Krol et al., 2012; Modic & Anderson, 2014). For example, Bravo-Lillo et al. (2011a) argued that warning messages should provide information about the potential consequences of sharing personal information with others because many non-experts do not fully understand how sharing personal information could affect them. Similarly, Bartsch et al. (2013) argued that warning messages should provide information about threat probability because non-experts do not fully understand how susceptible they are to threats.

That is a reasonable tactic because non-experts think differently than experts about cybersecurity (Asgharpour et al., 2007; Bartsch & Volkamer, 2013; Bravo-Lillo et al., 2011a; Theofanos et al., 2017). For example, non-experts think about cybersecurity in more abstract ways than experts (Bartsch & Volkamer, 2013), are less likely than experts to think about topics such as information security (Bravo-Lillo et al., 2011a) or risk factors for and consequences of threats (Bartsch & Volkamer, 2013), are less likely than experts to think they can protect themselves (Bartsch & Volkamer, 2013; Theofanos et al., 2017), are more likely than experts to think Web sites can be trusted to protect users' cybersecurity (Theofanos et al., 2017), and are more likely than experts to think about whether a Web site looks professional when deciding whether it is trustworthy (Bravo-Lillo et al., 2011a).

Perhaps as a result, non-experts sometimes make the conscious decision to *not* protect themselves from threats (Kang et al., 2015; Renaud et al., 2014; Theofanos et al., 2017; Vaniea et al., 2014; Weirich & Sasse, 2001; Wu & Zappalla, 2018). For example, non-experts have decided not to guard their passwords (Weirich & Sasse, 2001), e-mail (Renaud et al., 2014) or online privacy/cybersecurity (Kang et al., 2015; Theofanos et al., 2017), to not install operating system or application updates (Ion et al., 2015; Vaniea et al., 2014), and to not use encryption (Wu & Zappalla, 2018) or two-factor authentication (Ion et al., 2015).

Such choices create major security vulnerabilities. Therefore, it is critically important to understand why non-experts choose to *not* protect themselves from threats, and assess whether recommendations regarding designing warning messages adequately address why non-experts do so.

Toward that end, we synthesized relevant literature to 1) investigate why non-experts choose to *not* protect themselves from threats, and 2) catalog warning message recommendations that aim to influence how non-experts think about threats. Armed with that information, we then 3) evaluated whether the cataloged warning message recommendations adequately addressed the reasons why non-experts choose to *not* protect themselves from threats, and 4) discussed implications for future research.

CONTACT Keith S. Jones keith.s.jones@ttu.edu Psychological Sciences Department, Texas Tech University, Lubbock, TX 79409, USA

Thus, the present review makes two important contributions. First, it is the first to examine the reasons why non-experts choose to not protect themselves from threats. Second, it is the first to evaluate whether existing warning message recommendations that aim to influence how non-experts think about threats adequately addressed those reasons.

1.1. Organizational scheme

To accomplish our goal, we needed a scheme around which quite different literatures could be organized. We ultimately decided to organize research findings around the 5 elementary components of the Technology Threat Avoidance Theory (TTAT; Liang & Xue, 2009), p. 1) perceived susceptibility, 2) perceived severity, 3) perceived effectiveness, 4) perceived costs, and 5) self-efficacy. Those elements refer to users' thoughts regarding how 1) likely it is that the threat is real (perceived susceptibility), 2) harmful is the threat (perceived severity), 3) effective are threat countermeasures (perceived effectiveness), 4) physically and cognitively demanding are the relevant threat countermeasures (perceived costs), and 5) successfully can they implement relevant countermeasures (self-efficacy).

The decision to organize literatures around TTAT was not made a priori. Rather, we employed TTAT as our organizational scheme because all-but-one of the themes that emerged from our research syntheses aligned with the 5 elementary components of TTAT. We discussed the lone exception in a separate section.

To be clear, it was not our goal to evaluate TTAT. Our use of TTAT's elements as an organizational scheme should not be construed as an argument that non-experts' thinking when choosing to *not* protect themselves from threats is consistent with TTAT.

1.2. Overview

This paper is organized into separate sections. In the first, we discuss our method for finding and evaluating papers to include in the review. In the second, we present our synthesis of the literature concerning why non-experts choose to *not* protect themselves from threats. In the third, we present our synthesis of the literature concerning warning message recommendations that aim to influence how non-experts think about threats. In the fourth, we discuss whether those warning message recommendations adequately address the reasons why non-experts choose to *not* protect themselves from threats, and the associated implications. In the fourth, we discuss ideas for future research.

2. Method

To ensure a complete and thorough survey of the available literature, the databases of the ACM Digital Library and Google Scholar were queried using combinations of the search terms "mental model", "end user", "cyber threat", "web attack", "risk communication", and "online privacy". To be included in the evaluation stage, articles had to meet the following criteria: pertain to end-users, AND pertain to mental models of cyber threats of online privacy AND/OR pertain to warnings/risk communication in the cyber security domain. For each article that met the criteria, a backward and a forward search were performed to locate other articles that met the criteria that were cited in the found paper or that cited the found paper, respectively. Ninety-three papers were found concerning mental models of cyber security, risk communication using mental models of cybersecurity and recommendations for designing risk communication. These papers' range of publication date was 1978 to 2018.

We then evaluated those articles to ensure they discussed concrete reasons why people do not exhibit secure behaviors or discussed warning message recommendations aimed at influencing how non-experts think about threats. An example of a concrete reason is people not updating software because they thought the software would change and they would need to relearn how to work it (Vaniea et al., 2014). An example of a warning message recommendation aimed at influencing how non-experts think about threats is warning messages should provide information on the probability of a threat to encourage users to think the threat is real (Bartsch et al., 2013; Hardee et al., 2006; Herley, 2009; Krol et al., 2012). If an article included a concrete reason why people do not exhibit secure behaviors or a warning message recommendation aimed at influencing how non-experts think about threats, then the article was included in the current paper. If no reasons for users' behavior or warning message recommendations were provided, the article was not relevant to our paper and was not included. Eighteen articles met this criteria for user behavior and 11 articles met this criteria for warning message recommendations and were included in the synthesis.

3. Why do non-experts decide to *not* protect themselves from threats?

In this section, we describe research findings concerning why non-experts choose to *not* protect themselves from threats. Those findings came from two different types of studies: those that 1) directly asked non-experts to explain why they chose to not exhibit security conscious behaviors (Kang et al., 2015; Renaud et al., 2014; Theofanos et al., 2017; Vaniea et al., 2014; Weirich & Sasse, 2001; Wu & Zappalla, 2018), and 2) arrived at such explanations through less direct means, e.g., observing participants' behavior, such as entering a Web site after receiving a warning message, and asking participants to reflect on that behavior (Dourish et al., 2003; Hardee et al., 2006; Kauer et al., 2012; Prettyman et al., 2015; Sasse et al., 2001; Ur et al., 2016; Wash, 2010).

3.1. Threat appraisal: Perceived susceptibility

Non-experts who choose to *not* protect themselves think 2 things related to their perceived susceptibility. First, non-experts think they are not likely to be targeted because they often think they are not wealthy or important enough to warrant being attacked, i.e., they are not "big fish" (Kang et al., 2015; Kauer et al., 2013; Prettyman et al., 2015; Renaud et al., 2014; Sasse et al., 2001; Theofanos et al., 2017; Ur et al., 2016; Wash, 2010; Wash & Rader, 2015; Weirich &

Sasse, 2001), and sometimes think threats do not target individuals (Kauer et al., 2013; Wash, 2010). Regarding the latter, non-experts thought threats only target organizations so as to access large databases (Wash, 2010) or generate publicity or justice (Kauer et al., 2013). Second, non-experts sometimes think they do not have to protect themselves from threats because the systems with which they interact are inherently secure (Renaud et al., 2014). For example, non-experts reported that they did not encrypt e-mail because e-mail systems have strong security (Renaud et al., 2014). Collectively, these results suggest non-experts do not think they are very susceptible to cybersecurity threats.

3.2. Threat appraisal: Perceived severity

Non-experts who choose to *not* protect themselves think 2 things related to perceived severity. First, non-experts sometimes think they do not care whether someone violated their privacy (Kang et al., 2015). Second, non-experts sometimes think they have nothing to hide (Kang et al., 2015; Renaud et al., 2014; Wu & Zappalla, 2018), so cybersecurity threats could not harm them (Renaud et al., 2014; Sasse et al., 2001; Viseu et al., 2004; Weirich & Sasse, 2001). Such perspectives likely reflect an incomplete understanding of how attackers can leverage seemingly innocuous information. Collectively, these results suggest non-experts do not think cybersecurity threat consequences are very severe.

On a related note, non-experts who observed an SSL warning, but did not understand it, sometimes reported that they would ignore the warning and log into the Web site anyway (Kauer et al., 2012). Such behavior suggests that, in the absence of information about perceived severity, non-experts may not think about potential consequences of a threat.

3.3. Coping appraisal: Perceived effectiveness

Non-experts who choose to *not* protect themselves think 2 things related to perceived effectiveness. First, non-experts sometimes think that they have no real control over their privacy or security (Prettyman et al., 2015). Second, non-experts sometimes think that attackers will always be one step ahead of them (Dourish et al., 2003) and can always find a way to access what they want (Weirich & Sasse, 2001). Collectively, these results suggest non-experts do not consider cybersecurity threat countermeasures to be particularly effective, and have a generally fatalistic attitude (Prettyman et al., 2015).

3.4. Coping appraisal: Perceived costs

Non-experts who choose to *not* protect themselves think 2 things related to perceived costs. First, non-experts often think actions to protect themselves are an inconvenient distraction from the task at hand (Dourish et al., 2003; Hardee et al., 2006; Kang et al., 2015; Sasse et al., 2001) and negatively affect their productivity (Vaniea et al., 2014). For example, non-experts sometimes think operating system or application updates will force them to relearn how to use the software (Vaniea et al., 2014). To avoid such disruptions, those non-experts simply do not install software updates, especially when the software is not used frequently and functions properly without the update (Vaniea et al., 2014). Second, non-experts sometimes think tools that they would use to protect themselves are not effective and have poor usability (Kang et al., 2015). For example, those non-experts reported that search engines that are designed to protect one's online privacy are less effective and usable than mainstream search engines such as Google (Kang et al., 2015). Collectively, these results suggest non-experts think threat countermeasures are costly.

3.5. Coping appraisal: Self-efficacy

Non-experts who choose to *not* protect themselves think 1 thing related to self-efficacy. Specifically, non-experts sometimes think they do not know much about cybersecurity (Theofanos et al., 2017) or, more specifically, that they do not know how to protect their cybersecurity (Kang et al., 2015). That suggests non-experts' self-efficacy regarding executing cybersecurity threat countermeasures is probably quite low.

3.6. Not my job

Non-experts who choose to *not* protect themselves frequently think 1 thing that falls outside the scope of TTAT. Specifically, non-experts frequently think it is someone else's job to protect their cybersecurity (Dourish et al., 2003; Gross & Rosson, 2007; Prettyman et al., 2015; Renaud et al., 2014; Theofanos et al., 2017), which has come to be known as the "Not My Job" perspective in the literature (Prettyman et al., 2015). Sometimes, non-experts point to another individual, such as a knowledgeable friend, family member, colleague, or roommate, who ensures their security by, for example, setting up their computer in a secure manner (Dourish et al., 2003). Other times, they point to organizations. For example, non-experts sometimes argued that it was their e-mail service provider's job to keep others out of their e-mail (Renaud et al., 2014), a Web site's responsibility to ensure its users' online privacy (Prettyman et al., 2015; Theofanos et al., 2017), or an online bank's responsibility to ensure its customers' security (Dourish et al., 2003).

It is unclear how this perspective affects non-experts' thinking regarding cybersecurity. One possibility is that non-experts who think that it is not their job to protect their cybersecurity simply do not think about it. Alternatively, it is possible that non-experts who hold that view think about cybersecurity but are less motivated and are less willing to expend effort to do so. In that case, those non-experts may exhibit characteristics similar to those of "security fatigue", such as simplifying the situation, pursuing the option that requires the least effort or best aligns with their current motivations, and acting impulsively (Stanton et al., 2016).

3.7. Thought co-occurrence

The preceding sections separately discuss factors related to why non-experts choose to *not* protect themselves from threats. It is important to note, however, that those factors

sometimes co-occur. Those co-occurrences can be instructive. Below, we discuss two studies in which non-experts provided multiple reasons why they chose to *not* protect themselves from threats.

Renaud et al. (2014) asked non-experts to explain why they did not encrypt their e-mails. Non-experts noted they were not important enough to attack, e-mail systems are secure, they have nothing to hide, no harm would come to them if someone did access their e-mail, private e-mails are not particularly critical, and it was not their job to secure their e-mail.

Vaniea et al. (2014) asked non-experts to explain why they do not install software updates. Non-experts noted software updates can change the user interface, which can hinder productivity, and they did not understand why it was necessary to install software updates when the software functioned correctly or was used infrequently.

Collectively, these findings suggest 3 things. First, non-experts in a given situation have multiple reasons for why they choose to *not* protect themselves. Those reasons probably interact with one another. Second, non-experts do not always consider all aspects of the situation when choosing a behavior that does not protect them. In Renaud et al. (2014), non-experts did not report considering anything related to countermeasures (i.e., perceived effectiveness, perceived costs, or self-efficacy). In Vaniea et al. (2014), non-experts did not report considering anything related to the threat (i.e., perceived susceptibility or perceived severity). As such, non-experts may choose to *not* protect themselves based on an incomplete understanding of the situation. Third, non-experts do not always have the same reasons for choosing a less secure behavior. Specifically, non-experts in Renaud et al. (2014) and Vaniea et al. (2014) offered very different reasons for why they choose to *not* encrypt e-mails or update software. As such, non-experts' reasons for not exhibiting good cybersecurity behaviors may be task-dependent.

3.8. Summary

Non-experts who choose to *not* protect themselves think some combination of the following: 1) the threat is probably not real (perceived susceptibility), 2) the threat would not be harmful (perceived severity), 3) threat countermeasures are probably not effective (perceived effectiveness), 4) it would be costly to implement threat countermeasures (perceived costs), 5) they cannot successfully implement threat countermeasures (self-efficacy), and 6) it is not their job to protect themselves (Not My Job). Table 1 summarizes these main findings.

Table 1. A summary of the reasons why non-experts who choose to *not* protect themselves do not exhibit relevant security behaviors.

Factor	Non-Experts' Reasons
Perceived Susceptibility	Non-experts who choose to *not* protect themselves think they are not worthy of an attack
	Non-experts who choose to *not* protect themselves think attackers do not target individuals but focus on organizations
Perceived Severity	Non-experts who choose to *not* protect themselves do not care if their privacy is violated through an attack
	Non-experts who choose to *not* protect themselves think they have nothing to hide so an attack cannot harm them
Perceived Effectiveness	Non-experts who choose to *not* protect themselves think they have no control of their security
	Non-experts who choose to *not* protect themselves think attackers are always thinking ahead of them and can attack no matter the measures they take to prevent it.
Perceived Costs	Non-experts who choose to *not* protect themselves think security behaviors affect their productivity and are inconvenient
	Non-experts who choose to *not* protect themselves think security measures are not user-friendly
Self-Efficacy	Non-experts who choose to *not* protect themselves think they do not know how to protect against attacks
Not My Job	Non-experts who choose to *not* protect themselves think it is someone else's responsibility to protect their security, either another individual or an organization

4. Warning message recommendations that aim to influence non-experts' thinking

In this section, we catalog warning message recommendations that aim to influence how non-experts think about threats. Those recommendations came from 2 different types of studies: those in which researchers 1) made educated guesses about what information users lacked, created new warning messages to provide that information, and tested whether those new warning messages led to safer cybersecurity behavior than the original warnings (Bartsch et al., 2013; Bravo-Lillo et al., 2011b; Krol et al., 2012; Modic & Anderson, 2014), and 2) examined users' understanding of cybersecurity and made recommendations intended to ensure that warning messages align with users' understanding (Bartsch & Volkamer, 2013; Hardee et al., 2006; Kauer et al., 2012).

4.1. Threat appraisal: Perceived susceptibility

Researchers made 2 recommendations related to influencing how non-experts think about perceived susceptibility. First, warning messages should describe users' actions (Bartsch et al., 2013). For example, a warning message related to a spoofing attack should note users are entering their account number and PIN into what appears to be their bank's Web site (Bartsch et al., 2013). That way, non-experts may think the threat will affect them personally, which should encourage them to protect themselves (Bartsch et al., 2013; Kauer et al., 2012). Second, warning messages should include information about attack probability (Bartsch et al., 2013; Hardee et al., 2006; Herley, 2009; Krol et al., 2012). For example, Krol et al. (2012) argued warning messages should include statements such as " … It is highly probable that this PDF is malicious … " (pg. 3). That way, non-experts may consider the threat to be real.

On a related note, Hardee et al. (2006) argued that information about attack probability should be provided in combination with information about attack severity. For example, an e-mail from an unknown sender that contains a link could produce a warning that describes the information an attacker can gain if the user clicks on the link, the actions the attacker can take with the information entered into the linked Web site (attack severity), and the likelihood the e-mail is a phishing e-mail (attack probability). That way, non-experts can fully understand risk.

4.2. Threat appraisal: Perceived severity

Researchers made 2 recommendations related to influencing how non-experts think about perceived severity. First, warning messages should use color to represent threat severity (Ibrahim et al., 2010; Silic et al., 2017). For example, in the United States, red can be used in warning messages that describe financial consequences and orange can be used in warnings that describe consequences that are perceived to be less severe (Ibrahim et al., 2010). That way, non-experts may better understand threat severity. Second, warning messages should include information about threat consequences (Bartsch & Volkamer, 2013; Bartsch et al., 2013; Bravo-Lillo et al., 2011b; Hardee et al., 2006; Kauer et al., 2012; Krol et al., 2012; Modic & Anderson, 2014). For example, Modic and Anderson (2014) argued warning messages should clearly convey potential negative outcomes of the current situation. That way, non-experts can conceptualize the situation more concretely (Bartsch et al., 2013), which should enable a more complete understanding of threat severity.

On a related note, researchers have provided recommendations regarding how threat consequences should be described. Specifically, consequence descriptions should mention objects or information the attack will affect (Bravo-Lillo et al., 2011a), use non-technical language (Modic & Anderson, 2014), make clear how the non-expert will be personally affected (Bartsch et al., 2013; Kauer et al., 2012), and, when appropriate, mention the potential to lose money, property, or both (Hardee et al., 2006).

4.3. Coping appraisal: Perceived effectiveness

Researchers made 1 recommendation related to influencing how non-experts think about perceived effectiveness. Specifically, warning messages should provide users with specific instructions about how to avoid the threat they face (Bravo-Lillo et al., 2011a). For example, a warning message could recommend a user delete an e-mail with a potential phishing link.

It is important to note, however, that instructing users about how to avoid a threat may not address perceived effectiveness. It is one thing to understand the steps that must be taken to prevent an attack; it is another to perceive that those steps will successfully counter the threat.

4.4. Coping appraisal: Perceived costs

Researchers made 1 recommendation related to influencing how non-experts think about perceived costs. Specifically, warnings should directly contrast potential losses from the attack with estimates of how much time will be required to implement the recommended actions to prevent the attack (Hardee et al., 2006; Herley, 2009). For example, a warning to update anti-virus software should include the amount of time needed to update the software and the potential consequences of a virus attack, such as needing to buy a new computer because the virus damaged the current device (Hardee et al., 2006). That way, non-experts can better perceive the costs associated with threat countermeasures.

Please note, however, that this recommendation has not been empirically tested. Thus, it remains to be seen whether following it leads to safer cybersecurity behavior.

4.5. Coping appraisal: Self-efficacy

Researchers made 1 recommendation related to self-efficacy. Specifically, warning messages should provide users with information about what their response accomplished once they respond to the warning message (Ibrahim et al., 2010).

To increase self-efficacy, one must attempt the task and succeed (Bandura, 1994). Therefore, self-efficacy will not increase simply by providing users with specific instructions about how to avoid the threat they face. Rather, users must execute those instructions and receive feedback that their actions prevented the threat.

That said, it is presently unclear how warning messages should provide such feedback. One possibility would be to provide users with a follow-up message indicating their actions successfully prevented the threat. Providing such follow-up messages could increase non-experts' self-efficacy. However, providing such follow-up messages would also further disrupt non-experts' workflow, likely frustrating them. If so, then implementing such follow-up messages may not have a net positive effect on users, and an alternative means for providing feedback would be needed.

4.6. Complications associated with assessing the effectiveness of individual recommendations

The preceding sections discussed individual recommendations. It is important to note, however, that all of the experiments that compared redesigned warnings against standard warnings implemented *sets* of recommendations (Bartsch et al., 2013; Bravo-Lillo et al., 2011b; Krol et al., 2012; Modic & Anderson, 2014). For example, Bartsch et al. (2013) applied the following guidelines when redesigning their warnings: 1) describe the user's intention, 2) provide a headline that conveys attack probability, and 3) describe the potential personal consequences of the attack. As such, their redesigned warnings included information related to perceived susceptibility (i.e., attack probability and personalizing the attack) and severity (i.e., consequences). Their results revealed their redesigned warnings led to safer cybersecurity behavior than standard warnings. However, it is unclear what exactly led to safer cybersecurity behavior because they implemented a *set* of guidelines. Were some of the guidelines unnecessary? Did certain guidelines influence cybersecurity behavior more so than others? Unfortunately, existing experiments comparing redesigned warnings to standard warnings cannot answer such questions.

4.7. Summary

Researchers have proposed 7 recommendations regarding how warning messages should be designed so as to influence how non-experts think about threats. Specifically, warning messages should 1) describe users' actions (perceived susceptibility), 2) include information about threat probability

(perceived susceptibility), 3) use color to represent threat severity (perceived severity), 4) include information about threat consequences (perceived severity), 5) provide users with specific instructions about how to avoid the threat (perceived effectiveness), 6) directly contrast potential losses from the attack with estimates of how much time will be required to implement the recommended actions to prevent the attack (perceived costs), and 7) provide users with information about what their response accomplished once they respond to the warning message (self-efficacy). Table 2 summarizes these main findings.

5. Do warning message recommendations address why certain non-experts do not protect themselves?

In this section, we discuss whether warning message design recommendations that aim to influence how users think about cybersecurity threats address the specific reasons why certain non-experts choose to *not* exhibit security behaviors.

5.1. Threat appraisal: Perceived susceptibility

Non-experts who choose to *not* protect themselves think a) it is unlikely they will be targeted (Kang et al., 2015; Kauer et al., 2013; Prettyman et al., 2015; Renaud et al., 2014; Sasse et al., 2001; Theofanos et al., 2017; Ur et al., 2016; Wash, 2010; Weirich & Sasse, 2001), and b) systems with which they interact are inherently secure (Renaud et al., 2014). Therefore, they do not think they are very susceptible to threats.

Current warning message recommendations related to influencing how non-experts think about threat susceptibility concerned a) mentioning users' intentions (Bartsch & Volkamer, 2013), and b) conveying attack probability (Bartsch et al., 2013; Hardee et al., 2006; Krol et al., 2012). The former aims to encourage non-experts to think about the threat affecting them personally; the latter aims to convince non-experts that the threat is real.

Neither of those recommendations directly address the reasons why non-experts who choose less secure behaviors think they are not very susceptible to cybersecurity threats. Specifically, those recommendations do not appear to counter non-experts' thoughts that they are not important or wealthy enough to warrant being targeted, or their thoughts that systems they use are inherently secure. As such, it is possible that non-experts' blanket beliefs about their susceptibility may outweigh the conveyed information about, for example, attack probability. In essence, some non-experts may read and understand the warning but dismiss it as irrelevant to them because they "know" they are not the kind of person who would be targeted, and that even if they were targeted, the system they are using is secure.

Table 2. A summary of the warning message recommendations that aim to influence how non-experts think about threats.

Factor	Warning Message Recommendation(s)
Perceived Susceptibility	Describe users' actions to provide the threat in context of users' behavior
	Include information about attack probability (in combination with attack severity)
Perceived Severity	Use color to indicate the severity of the attack (e.g., red = severe)
	Provide information about potential consequences of the attack
Perceived Effectiveness	Provide the steps to avoid the attack
Perceived Costs	Compare the time needed to implement the security measure to the consequences of the attack
Self-Efficacy	Provide information about what the user's response to the warning message accomplished

5.2. Threat appraisal: Perceived severity

Non-experts who choose to *not* protect themselves think a) they do not care whether someone violates their privacy (Kang et al., 2015), and b) they have nothing to hide (Kang et al., 2015; Renaud et al., 2014; Wu & Zappalla, 2018), so cybersecurity threats cannot harm them (Renaud et al., 2014; Sasse et al., 2001; Viseu et al., 2004; Weirich & Sasse, 2001). Therefore, they do not think cybersecurity threats are severe.

Current warning message recommendations related to influencing how non-experts think about threat severity concerned a) using color to represent threat severity (Ibrahim et al., 2010; Silic et al., 2017), and b) including information about threat consequences (Bartsch & Volkamer, 2013; Bartsch et al., 2013; Bravo-Lillo et al., 2011b; Hardee et al., 2006; Kauer et al., 2012; Krol et al., 2012; Modic & Anderson, 2014). The latter aims to encourage non-experts to think about the threat in concrete terms (Bartsch et al., 2013).

Implementing those recommendations may help to convince non-experts who do not take actions to prevent attacks that cybersecurity threats can harm them. We stress *may help* because providing information about threat consequences does not necessarily address that non-experts who choose to not protect themselves think they do not care whether someone violates their privacy or that losing control over their personal information could harm them. For example, a warning message indicating that noncompliance could result in attackers accessing one's personal information provides information about threat consequences but does not do so in a manner that specifically addresses a lack of concern for protecting one's privacy or convinces one that losing control of that personal information could be harmful. Warning messages that address those thoughts when discussing threat consequences should be most impactful.

5.3. Coping appraisal: Perceived effectiveness

Non-experts who choose to *not* protect themselves think a) they have no real control over their privacy or security (Prettyman et al., 2015), and b) attackers will always be one step ahead of them (Dourish et al., 2003) and can always find a way to access what they want (Weirich & Sasse, 2001). These thoughts suggest they do not think cybersecurity threat countermeasures are particularly effective.

The current warning message recommendation related to influencing how non-experts think about perceived effectiveness suggests providing users with specific instructions about how to avoid the threat they face (Bravo-Lillo et al., 2011a).

The goal presumably being to ensure that non-experts understand how to counter the threat.

Implementing that recommendation may benefit non-experts who choose to *not* protect themselves because they often express that they do not understand how to protect themselves from threats (Kang et al., 2015). However, as noted earlier, understanding the steps that must be taken to prevent an attack is not the same as perceiving that those steps will prevent the attack. For example, a non-expert who thinks they have no real control over their privacy or security and that attackers can always find a way to access what they want will probably not think differently after reading instructions regarding how to avoid the threat. Therefore, implementing that recommendation will likely not lead non-experts to properly calibrate their perceptions of countermeasure effectiveness.

5.4. Coping appraisal: Perceived costs

Non-experts who choose to *not* protect themselves think a) actions to protect themselves are an inconvenient distraction from the task at hand (Dourish et al., 2003; Hardee et al., 2006; Kang et al., 2015; Sasse et al., 2001) and negatively affect their productivity (Vaniea et al., 2014), and b) tools that they would use to protect themselves are not effective and have poor usability (Kang et al., 2015). As such, they presumably think threat countermeasures are too costly to implement.

The current warning message recommendation related to influencing how non-experts think about perceived costs suggests directly contrasting potential losses from the threat with estimates of how much time will be required to implement the recommended actions to prevent the threat (Hardee et al., 2006; Herley, 2009). The goal being to enable non-experts to weigh the pros and cons of compliance.

That recommendation does not directly address the reasons why non-experts who choose to *not* protect themselves think cybersecurity threats are too costly. Therefore, implementing that recommendation may not always have the desired effect on non-experts who choose to *not* protect themselves. For example, non-experts reported that they chose to not update their software because updates sometimes include user interface changes, which can negatively affect their productivity (Vaniea et al., 2014). For those individuals, it will not be sufficient to simply indicate that the software update will greatly increase system security and will only take a few seconds. Rather, it will likely be necessary to also assuage their concerns about user interface changes. Otherwise, the warning message will not directly address the specific concerns they have about the perceived costs associated with that software update, and will likely be ignored.

5.5. Coping appraisal: Self-efficacy

Non-experts who choose to *not* protect themselves think they do not know much about cybersecurity (Theofanos et al., 2017) or, more specifically, that they do not know how to protect their cybersecurity (Kang et al., 2015). Therefore, their self-efficacy regarding executing cybersecurity threat countermeasures is probably quite low.

The current warning message recommendation related to influencing non-experts' self-efficacy suggested that warning messages should provide users with information about what their response accomplished once they respond to the warning message (Ibrahim et al., 2010). The goal being to allow non-experts to understand what they accomplished.

Implementing that recommendation could increase non-experts' self-efficacy, which increases when one successfully completes the task (Bandura, 1994). As noted earlier, though, it is currently unclear how to implement that recommendation without further disrupting non-experts' workflow, which may increase frustration.

5.6. Not my job

Non-experts who choose to *not* protect themselves often think it is not their job to do so (Dourish et al., 2003; Gross & Rosson, 2007; Prettyman et al., 2015; Renaud et al., 2014; Theofanos et al., 2017). Rather, they think that is another individual's job (Dourish et al., 2003), or an organization's job (Dourish et al., 2003; Prettyman et al., 2015; Renaud et al., 2014; Theofanos et al., 2017).

None of the current warning message design recommendations specifically addressed non-experts' thinking that it is someone else's job to protect them from cybersecurity threats. This is a critical omission because such an overarching belief may override other efforts to help non-experts exhibit behaviors that prevent against cyber-attacks. That is, efforts to convince non-experts that they face a severe threat but can effectively counter that threat with minimal effort, may be moot if non-experts simply ignore that information because it is not their job to try to prevent the threat.

6. Conclusions

Researchers have proposed 7 recommendations regarding how warning messages should be designed so as to influence how non-experts think about threats. The results of the preceding analysis suggest that, for the most part, those recommendations do not address the reasons why non-experts' do not attempt to prevent cyber-attacks (see Table 3 for a summary). Therefore, the present analysis reveals a critically important insight, that is, it is unlikely that implementing warning messages that reflect those recommendations will be enough to convince those non-experts to protect themselves.

To be clear, that is not meant to imply that designing warning messages that reflect those recommendations would have no effect whatsoever. Most of those recommendations have empirical support (Bartsch et al., 2013; Bravo-Lillo et al., 2011b; Krol et al., 2012; Modic & Anderson, 2014). Therefore, we know that they encourage safe cybersecurity behavior. Given the preceding analysis, though, it is unlikely that those positive effects stem from convincing non-experts, who would otherwise choose a less secure option, to protect themselves. Rather, those positive effects likely reflect influencing how other types of non-experts think.

If so, then that may help to explain why redesigning warning messages to reflect these recommendations significantly

Table 3. The reasons certain non-experts give for not protecting themselves from threats, and whether current warning message design recommendations address those reasons.

Factor	Non-Experts' Reasons	Do Recommendations Address Reasons?
Perceived Susceptibility	Non-experts who choose to *not* protect themselves think they are not worthy of an attack	No, relevant recommendations suggest mentioning users' intentions and conveying attack probability. Neither address that these non-experts think they are not important enough to be attacked
	Non-experts who choose to *not* protect themselves think attackers do not target individuals but focus on organizations	No, relevant recommendations suggest mentioning users' intentions and conveying attack probability. Neither address that these non-experts think they will not be attacked because attackers target organizations rather than individuals
Perceived Severity	Non-experts who choose to *not* protect themselves do not care if their privacy is violated	No, relevant recommendations suggest using color to represent threat severity and including information about threat consequences. Neither directly addresses that these non-experts do not care if their privacy is violated
	Non-experts who choose to *not* protect themselves think they have nothing to hide so an attack cannot harm them	Somewhat, relevant recommendations suggest using color to represent threat severity and including information about threat consequences. Implementing the latter may help to convince non-experts that cybersecurity threats can harm them
Perceived Effectiveness	Non-experts who choose to *not* protect themselves think they have no control of their security	No, the relevant recommendation suggests providing users with specific instructions about how to avoid the threat. That does not address that these non-experts think they have no control over their security
	Non-experts who choose to *not* protect themselves think attackers are always thinking ahead of them and can attack no matter the measures they take to prevent it	No, the relevant recommendation suggests providing users with specific instructions about how to avoid the threat. That does not address that these non-experts think attackers can attack them regardless of the countermeasures they may employ
Perceived Costs	Non-experts who choose to *not* protect themselves think security behaviors affect their productivity and are too inconvenient	No, the relevant recommendation suggests directly contrasting potential losses from the threat with estimates of how much time will be required to implement the recommended actions to prevent the threat. That will likely do little to convince these non-experts that countermeasures are too inconvenient
	Non-experts who choose to *not* protect themselves think security tools are not user-friendly enough	No, the relevant recommendation suggests directly contrasting potential losses from the threat with estimates of how much time will be required to implement the recommended actions to prevent the threat. That will likely do little to convince these non-experts that countermeasures are not user-friendly enough
Self-Efficacy	Non-experts who choose to *not* protect themselves think they do not know how to protect against attacks	Yes, the relevant recommendation suggests providing users with information about what they accomplished once they respond to the warning message. That could increase self-efficacy if these non-experts are told that their actions successfully thwarted the attack
Not My Job	Non-experts who choose to *not* protect themselves think it is someone else's responsibility to protect their security, either another individual or an organization	No, none of the current warning message design recommendations specifically addressed non-experts thinking that it is someone else's job to protect them from cybersecurity threats

improves user compliance (Bartsch et al., 2013; Bravo-Lillo et al., 2011b; Modic & Anderson, 2014; c.f., Krol et al., 2012), but overall levels of compliance sometimes remain lower than desired. For example, Bartsch et al. (2013) reported that users complied with 17% of original warnings and 46% of redesigned warnings. That is a 29% increase in compliance, which is noteworthy. However, overall compliance is still less than desirable, i.e., users not complying with over 50% of warnings, and that may be because the redesigned warning messages may not have addressed why certain non-experts choose to not comply with warning messages.

By determining that existing warning message design recommendations do not adequately address the reasons why non-experts' choose to *not* protect themselves from threats, the present analysis reveals another critically important insight, that is, researchers must turn their attention to understanding why those non-experts think those things, and how to best counteract those thoughts. Specific potential research ideas are discussed in the following section.

6.1. Future research concerning non-experts' overarching beliefs

Non-experts who choose to *not* protect themselves from threats expressed three overarching beliefs: 1) they are not likely to be targeted, 2) there is nothing they can do to prevent cyber-attacks, and 3) it is not their job to protect their cyber-security. Collectively, those beliefs should greatly decrease one's motivation to protect themselves from threats.

Therefore, it will likely be quite difficult to motivate non-experts to protect themselves from cybersecurity threats as long as they hold such beliefs. For instance, even the most carefully crafted warning messages are likely to be ignored if one thinks it is not their job to protect themselves from cybersecurity threats. Therefore, it will be necessary to shift non-experts who choose to not protect themselves away from these ways of thinking.

To be clear, we are not suggesting that non-experts need to become experts. There is considerable evidence that users can act adaptively without having a complete or completely accurate understanding of the situation (Garg & Camp, 2012; Wash, 2010). As such, we are suggesting that non-experts' thinking regarding those overarching beliefs needs to shift to the point where they can act adaptively.

To do so, we need to better understand why non-experts develop those beliefs. This is especially true for the latter two beliefs, about which we know fairly little. In addition, we need to understand how they affect non-experts' motivation to exhibit safe cybersecurity behaviors. Do non-experts who hold these overarching beliefs exhibit any cybersecurity behaviors? Does the answer to that question depend on which view, or set of views, non-experts hold? Answers to such questions will help researchers to develop effective ways to counteract the effects of such beliefs.

That said, it may not be possible to fully address those three overarching beliefs with warning messages. For example, it may not be feasible to change a non-expert's belief about whether it is their job to protect their cybersecurity through a warning message about a given attack. Instead, addressing these three overarching beliefs may require a two-pronged strategy.

The first prong would be actions taken to establish a cybersecurity safety culture within the organization. For example, anonymous reporting of errors in healthcare allows for more communication about errors (Halligan & Zecevic, 2011). One way to apply this approach to cybersecurity is to allow users to report when they were a victim of an attack. This reporting would provide more information about attacks that are currently occurring. This information could then be distributed by the company to other users in hopes of preventing future users from becoming a victim. This open communication can help non-experts realize their actions can protect their device, educate them on how to prevent these attacks, and perhaps include some modeling, which could increase self-efficacy (Bandura, 1994). Another way to establish a safety culture is to emphasize that everyone has an equal role in protecting against these attacks. In aviation, crew resource management was implemented, which improved the teamwork in the cockpit and caused both pilots and copilots to be responsible for preventing human errors (Helmreich et al., 1999). This idea can be applied to cyber-security by emphasizing that users, as well as organizations, are responsible for cyber-security. Organizations, such as banks, can inform users that cybersecurity is strengthened by the users' actions as well as the organization's actions. If an organization that users expect to protect them provides this information, users may consider taking responsibility for their own security.

Some organizations and governments have implemented awareness training programs to encourage such safety cultures (Abawajy, 2014; Bada et al., 2015; McCoy & Fowler, 2004). These programs aim to make people aware of certain attacks and instruct people on good security behaviors (Abawajy, 2014; Bada et al., 2015; McCoy & Fowler, 2004). Certain aspects of these programs could affect the beliefs non-experts have about cybersecurity, ultimately affecting their motivation to protect against cyber threats. For example, providing non-experts with information on how to protect against specific threats could affect their belief that there is nothing they can do to prevent an attack. Additionally, these programs can create a cybersecurity safety culture that can lead people to feel responsible for protecting an organization's and their own assets, which could change their belief that they are not responsible for cybersecurity (Abawajy, 2014). However, only certain methods of awareness programs may address non-experts' belief that they are not likely to be targeted. Abawajy (2014) mentioned that awareness programs are sometimes provided through a presentation with a facilitator in which people may discuss their experiences with cyber-security. If people share their stories of being attacked or the facilitator shares examples of attacks that affected fellow employees, then people may change their belief that they cannot be targeted. Not all programs include this information. Consistent with the findings of Abawajy (2014) and Shaw et al. (2009), multiple methods of presenting awareness programs (e.g., text, video, presentations) may be needed

to cover all information that would change these three overarching beliefs held by non-experts and foster a better cybersecurity culture.

The second prong would be to reinforce those messages, to the extent possible, within individual warning messages that non-experts may experience. For example, the text in a warning message can emphasize that user actions can compromise security beyond the security imposed by an organization. This warning can remind users that they are also responsible for their security. Developing such a two-pronged solution will require considerable research.

6.2. Future research concerning other factors

Considerable research is also needed to better understand factors that influence non-experts' thoughts that fall into the five elements of TTAT. By understanding non-experts' beliefs about these elements better, we can determine how to change non-experts' thinking on these elements and improve compliance with warning messages.

More questions need to be answered to gain more information about factors related to threat appraisal. For non-experts to be motivated to follow the recommended behavior in a warning message, they need to perceive themselves as susceptible to the threat. Thus, it will be important for research to address questions such as: why do some non-experts think systems are inherently secure, and how exactly does that influence their perceptions of susceptibility? Additionally, non-experts need to perceive a threat to be harmful to be motivated to comply with the warning message recommendation and exhibit the behavior. Some questions to ask regarding perceived severity are the following: Why do some non-experts think that cyber-attacks cannot hurt them? Is that grounded in assumptions they make about how accessed information can be used, and, if so, how do we go about changing those assumptions?

There is also a need for more research concerning coping appraisal that would allow for a better understanding of how to improve warning message compliance. One aspect of coping appraisal is perceived effectiveness or non-experts believing that the behavior being suggested by the warning will effectively prevent against the threat. To better understand how to improve perceived effectiveness, we can ask the following questions: what factors contribute to perceived effectiveness? Is there a linear or non-linear relationship between how much some non-experts know about cybersecurity countermeasures and their perceived effectiveness? In addition to believing counter measures are effective, non-experts need to think the cost incurred by performing the behavior is not greater than the benefits gained. To learn more about non-experts' perceived costs of security behaviors, the following question can be studied: what specific costs concern those non-experts when considering implementing a given countermeasure? Lastly, non-experts need to think they can carry-out the security behavior recommended by the warning message. The warning message literature does not have many recommendations for how to influence self-efficacy. Some questions to answer that may lead to more recommendations for improving self-efficacy are the following: what factors influence cybersecurity self-efficacy? Are non-experts' choices regarding whether to protect themselves task dependent, and, if so, on what task-related factors do those choices depend? Answering such questions should go a long way toward understanding how to design warning messages so as to encourage non-experts who would not otherwise protect themselves from cybersecurity threats to do so.

Acknowledgments

This research was supported by the National Science Foundation (NSF) under award # 1564293. Opinions, findings, and conclusions are those of the authors and do not necessarily reflect the views of NSF.

Disclosure of potential conflict of interest

No potential conflict of interest was reported by the author(s).

References

Abawajy, J. (2014, March). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

Asgharpour, F., Liu, D., & Camp, L. J. (2007). Mental models of security risks. In *International conference on financial cryptography and data security* (pp. 367–377). Springer.

Bada, M., Sasse, A. M., & Nurse, J. R. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? In *International conference on cyber security for sustainable society, coventry, United Kingdon* (pp. 118–131).

Bandura, A. (1994). Self-efficacy. In V. S. Ramachaudran Ed., *Encyclopedia of human behavior* (Vol. 4, pp. 71–81). Academic Press. (Reprinted in H. Friedman [Ed.], *Encyclopedia of mental health*. San Diego: Academic Press, 1998).

Bartsch, S., & Volkamer, M. (2013). Effectively communicate risks for diverse users: A mental-models approach for individualized security interventions. In M. Horbach (Ed.), *INFORMATIK 2013 – Informatik angepasst an Mensch, Organisation und Umwelt* (pp. 1971–1984). Gesellschaft für Informatik e.V.

Bartsch, S., Volkamer, M., Theuerling, H., & Karayumak, F. (2013). Contextualized web warnings, and how they cause distrust. In *International conference on trust and trustworthy computing* (pp. 205–222). Springer. https://doi.org/10.1007/978-3-642-38908-5_16

Bravo-Lillo, C., Cranor, L. F., Downs, J. S., & Komanduri, S. (2011a, March). Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy Magazine*, *9*(2), 18–26. https://doi.org/10.1109/MSP.2010.198

Bravo-Lillo, C., Cranor, L. F., Downs, J. S., Komanduri, S., & Sleeper, M. (2011b). Improving computer security dialogs. In *IFIP conference on human-computer interaction* (pp. 18–35). Springer.

Dourish, P., De La Flor, J. D., & Joseph, M. (2003). Security as a practical problem: Some preliminary observations of everyday mental models. In *Proceedings of CHI 2003 workshop on HCI and security systems*. ACM.

Garg, V., & Camp, J. (2012). End user perception of online risk under uncertainty. In *Proceedings of 45th Hawaii international conference on system sciences (HICSS)* (pp. 3278–3287). IEEE Computer Society. https://doi.org/10.1109/HICSS.2012.245.

Gross, J. B., & Rosson, M. B. (2007). Looking for trouble: Understanding end-user security management. In *Proceedings of the 2007 symposium on computer human interaction for the management of information technology (CHIMIT '07)*. ACM. https://doi.org/10.1145/1234772.1234786

Halligan, M., & Zecevic, A. (2011, February). Safety culture in healthcare: A review of concepts, dimensions, measures, and progress. *Quality and Safe Health Care*, *20*(4), 1–6. http://dx.doi.org/10.1136/bmjqs.2010.040964

Hardee, J. B., West, R., & Mayhorn, C. B. (2006, May). To download or not to download: An examination of computer security decision making. *Interactions*, *13*(3), 32–37. https://doi.org/10.1145/1125864.1125887

Helmreich, R. L., Merritt, A. C., & Wilhelm, J. A. (1999). The evolution of crew resource management training in commercial aviation. *International Journal of Aviation Psychology*, *9*(1), 19–32. https://doi.org/10.1207/s15327108ijap0901_2

Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. In *Proceedings of the 2009 workshop on new security paradigms workshop (NSPW '09)* (pp. 133–144). ACM.

Ibrahim, T., Furnell, S. M., Papadaki, M., & Clarke, N. L. (2010, August). Assessing the usability of end-user security software. In *International conference on trust, privacy and security in digital business* (pp. 177–189). Springer.

Ion, I., Reeder, R., & Consolvo, S. (2015). "… No one can hack my mind": Comparing expert and non-expert security practices. In *Eleventh symposium on usable privacy and security (SOUPS)* (pp. 327–346). ACM Press.

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). "My data just goes everywhere:" user mental models of the internet and implications for privacy and security. In *Symposium on Usable Privacy and Security (SOUPS)* (pp. 39–52). USENIX Association.

Kauer, M., Günther, S., Storck, D., & Volkamer, M. (2013). A comparison of American and German folk models of home computer security. In *International conference on human aspects of information security, privacy, and trust* (pp. 100–109). Springer.

Kauer, M., Pfeiffer, T., Volkamer, M., Theuerling, H., & Bruder, R. (2012). *It is not about the design-it is about the content! Making warnings more efficient by communicating risks appropriately*. GI-Edition – Lecture Notes in Informatics (LNI).

Krol, K., Moroz, M., & Sasse, M. A. (2012). Don't work. Can't work? Why it's time to rethink security warnings. In *2012 7th international conference on risk and security of internet and systems (CRiSIS)* (pp. 1–8). IEEE. https://doi.org/10.1109/CRISIS.2012.6378951

Liang, H., & Xue, Y. (2009, March). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, *33*(1), 71–90. https://doi.org/10.2307/20650279

McCoy, C., & Fowler, R. T. (2004). " You are the key to security" establishing a successful security awareness program. In *Proceedings of the 32nd annual ACM special interest group on university and college computing services (SIGUCCS) conference on user services* (pp. 346–349). ACM.

Modic, D., & Anderson, R. (2014, December). Reading this may harm your computer: The psychology of malware warnings. *Computers in Human Behavior*, *41*, 71–79. https://doi.org/10.1016/j.chb.2014.09.014

Prettyman, S. S., Furman, S., Theofanos, M., & Stanton, B. (2015). Privacy and security in the brave new world: The use of multiple mental models. In *International conference on human aspects of information security, privacy, and trust* (pp. 260–270). Springer International Publishing.

Renaud, K., Volkamer, M., & Renkema-Padmos, A. (2014). Why doesn't Jane protect her privacy? In E. De Cristofaro & S. J. Murdoch (Eds.), *Privacy enhancing technologies (PETS). Lecture notes in computer science* (pp. 8555). Springer.

Sasse, M. A., Bronstoff, S., & Weirich, D. (2001, July). Transforming the "Weakest Link": A human-computer interaction approach for usable and effective security. *BT Technology Journal*, *19*(3), 122–131. https://doi.org/10.1023/A:1011902718709

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009, January). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

Silic, M., Cyr, D., Back, A., & Holzer, A. (Eds.). (2017, March). Effects of color appeal, perceived risk and culture on users decision in presence of warning banner message. In *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016, September/October). Security fatigue. *IT Professional*, *18*(5), 26–32. https://doi.org/10.1109/MITP.2016.84

Theofanos, M. F., Stanton, B., Furman, S., Prettyman, S. S., & Garfinkel, S. (2017). Be prepared: How US government experts think about cybersecurity. In *Network and distributed system security symposium (NDSS)* (pp. 1–11). Information Society. https://doi.org/10.14722/usec.2017.23006

Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N., & Cranor, L. F. (2016). Do users' perceptions of password security match reality?. In *Proceedings of the 2016 CHI conference on human factors in computing systems* (pp. 3748–3760). ACM.

Vaniea, K. A., Rader, E., & Wash, R. (2014). Betrayed by updates: How negative experiences affect future security. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 2671–2674). ACM. https://doi.org/10.1145/2556288.2557275

Viseu, A., Clement, A., & Aspinall, J. (2004). Situating privacy online: Complex perceptions and everyday practices. *Information, Communication & Society*, *7*(1), 92–114. https://doi.org/10.1080/1369118042000208924

Wash, R. (2010). Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS)* (1–11). ACM Press.

Wash, R., & Rader, E. J. (2015). Too much knowledge? Security beliefs and protective behaviors among United States internet users. In *Proceedings of the symposium on usable privacy and security (SOUPS)* (pp. 309–325). ACM.

Weirich, D., & Sasse, M. A. (2001). Pretty good persuasion: A first step towards effective password security in the real world. In *Proceedings of the 2001 workshop on new security paradigms (NSPW '01)* (pp. 137–143). ACM.

Wu, J., & Zappalla, D. (2018). When is a tree really a truck? Exploring mental models of encryption. In *Proceedings of the fourteenth symposium on usable privacy and security (SOUPS)* (pp. 395–409). USENIX Association.

About the Authors

Keith S. Jones is an Associate Professor of Psychology at Texas Tech University. He received his PhD in Experimental Psychology with an emphasis on Human Factors Psychology from the University of Cincinnati in 2000.

Natalie R. Lodinger is a graduate student in the Texas Tech University Human Factors program.

Benjamin P. Widlus is a graduate student in the Texas Tech University Human Factors program.

Akbar Siami Namin is an Associate Professor of Computer Science at Texas Tech University. He received his PhD in Computer Science with an emphasis on Software engineering from the University of Western Ontario in 2008.

Rattikorn Hewett is a Professor of Computer Science at Texas Tech University. She received her PhD in Computer Science from Iowa State University in 1986.