10-2021

Impact of digital nudging on information security behavior: An experimental study on framing and priming in cybersecurity

Kavya SHARMA

Xinhui ZHAN

Fiona Fui-hoon NAH
Singapore Management University, fionanah@smu.edu.sg

Keng SIAU
Singapore Management University, klsiau@smu.edu.sg

Maggie X. CHENG

Citation

SHARMA, Kavya; ZHAN, Xinhui; NAH, Fiona Fui-hoon; SIAU, Keng; and CHENG, Maggie X.. Impact of digital nudging on information security behavior: An experimental study on framing and priming in cybersecurity. (2021). *Organizational Cybersecurity Journal*. 19, (1), 69-91.
Available at: https://ink.library.smu.edu.sg/sis_research/9526

Impact of digital nudging on information security behavior: an experimental study on framing and priming in cybersecurity

Kavya Sharma
World Wide Technology, St. Louis, Missouri, USA and
Missouri University of Science and Technology, Rolla, Missouri, USA
Xinhui Zhan
University of Oklahoma, Norman, Oklahoma, USA and
Missouri University of Science and Technology, Rolla, Missouri, USA
Fiona Fui-Hoon Nah and Keng Siau
City University of Hong Kong, Kowloon Tong, Hong Kong, and
Maggie X. Cheng
Illinois Institute of Technology, Chicago, Illinois, USA

Received 15 March 2021
Revised 11 May 2021
Accepted 11 June 2021

Abstract

Purpose – Phishing attacks are the most common cyber threats targeted at users. Digital nudging in the form of framing and priming may reduce user susceptibility to phishing. This research focuses on two types of digital nudging, framing and priming, and examines the impact of framing and priming on users' behavior (i.e. action) in a cybersecurity setting. It draws on prospect theory, instance-based learning theory and dual-process theory to generate the research hypotheses.

Design/methodology/approach – A 3 × 2 experimental study was carried out to test the hypotheses. The experiment consisted of three levels for framing (i.e. no framing, negative framing and positive framing) and two levels for priming (i.e. with and without priming).

Findings – The findings suggest that priming users to information security risks reduces their risk-taking behavior, whereas positive and negative framing of information security messages regarding potential consequences of the available choices do not change users' behavior. The results also indicate that risk-averse cybersecurity behavior is associated with greater confidence with the action, greater perceived severity of cybersecurity risks, lower perceived susceptibility to cybersecurity risks resulting from the action and lower trust in the download link.

Originality/value – This research shows that digital nudging in the form of priming is an effective way to reduce users' exposure to cybersecurity risks.

Keywords Cybersecurity, Framing, Priming, Digital nudging, Information security, User behavior

Paper type Research paper

1. Introduction

Information security risks are on the rise and social engineering attacks such as phishing are rapidly increasing (Carpenter, 2020; Thibodeaux, 2021). These risks and attacks pose

The authors acknowledge the support from the National Science Foundation (CNS/1537538) for this research.

Organizational Cybersecurity Journal: Practice, Process and People
Vol. 1 No. 1, 2021
pp. 69-91
Emerald Publishing Limited
e-ISSN: 2635-0289
p-ISSN: 2635-0270
DOI 10.1108/OCJ-03-2021-0009

significant challenges to organizations in keeping their data safe (Stephanidis *et al.*, 2019). IBM has reported that more than 95% of their security incidents were attributed to human errors (IBM Corporation, 2014). Similarly, data breaches at companies such as Equifax and Capital One were caused primarily by human errors (Bernard and Cowley, 2017; Yakencheck, 2019). Users play a critical role in identifying cybersecurity threats and preventing cybersecurity incidents (Stanton *et al.*, 2004) such as those associated with downloading documents or software from anonymous or unknown sources. Phishing attacks are the most common cyber threats to users and organizations. Phishing messages typically entice users to take risky cybersecurity actions by downloading uncertified software or visiting a malicious website. For example, a watering hole phishing attack takes place by infecting websites frequent by targeted users such that user information could be compromised when software is downloaded from these websites. Phishing attacks can also take place through other means, such as emails, tweets, phone calls or SMS. Therefore, it is critical to explore factors that can safeguard users' behavior and investigate ways to minimize users' exposure to cybersecurity risks.

The information systems (IS) security literature has examined user vulnerability to cyberattacks and explored individual differences and psychological factors, including cognitive limitations, personality traits, identity and other demographic factors (Shropshire *et al.*, 2015; Halevi *et al.*, 2013). Past research has also investigated the structural features of security warnings, suggesting that security behavior is influenced by active warnings (Akhawe and Felt, 2013), security cues (Smith *et al.*, 2016) and security messages (Chen *et al.*, 2015; Chong *et al.*, 2018; Rosoff *et al.*, 2013). User behavior plays a vital role in cybersecurity (McNeese *et al.*, 2012) and is affected by the decision environment and context (Wang *et al.*, 2019).

Nudge theory has been used to understand how people make decisions and, more importantly, how to improve people's thinking and decisions by the design of choices (Thaler and Sunstein, 2009). Human-computer interaction researchers further defined "digital nudging" as the use of specific information to "nudge" users into behaving in a predictable way (Schneider *et al.* 2018; Weinmann *et al.*, 2016). However, users' decision-making associated with digital nudging in the cybersecurity context is still largely unexplored. Hence, more research is warranted to overcome human factors and social engineering as the means leading to cybersecurity attacks. Specifically, in this paper, we examine the impact of two types of digital nudging, framing and priming, on users' information security behavior in a software download context. Thus, our research questions are:

RQ1. Does priming users to known instances of information security risks reduce their risk-taking behavior?

RQ2. Do positive and negative framing of information security messages regarding potential consequences of choices reduce users' risk-taking behavior?

This paper is organized as follows: Section 2 reviews the literature on digital nudging, framing, priming and user behavior in the cybersecurity context. Section 3 provides the theoretical foundation for the research by covering dual-process theory, prospect theory and instance-based learning theory, as well as presents the research hypotheses. Section 4 presents the research methodology. The data analysis and discussions of findings are presented in section 5 and section 6, respectively. Finally, section 7 concludes the paper with theoretical and practical implications as well as limitations and future research directions.

2. Literature review

2.1 Nudges in cybersecurity

Nudges are powerful and straight-forward strategies that change the architecture of choices to improve human decision-making. Nudges have been shown to be beneficial to decision-making in a variety of areas, including finance (Castleman and Page, 2016; Marx and Turner, 2019), healthcare (Dubov and Phung, 2015), education (Damgaard and Nielsen, 2018) and e-commerce (Dennis *et al.*, 2020). A nudge is any aspect of the choice architecture that alters people's behavior (Thaler and Sunstein, 2009). For example, in an e-commerce study, it was found that the price of a similar product available elsewhere can influence people's willingness to buy that product from an e-commerce site (Krishna *et al.*, 2006). Dennis *et al.* (2020) termed this phenomenon as semantic priming, which refers to people's tendency to use a related product as an initial anchor in the purchase decision-making process.

Researchers in the security and privacy area have been exploring ways to nudge users to better their security decisions (Renaud and Zimmermann, 2018; Cooper *et al.*, 2020). For instance, Peer *et al.* (2020) developed a personalized approach that analyzed individual differences in decision-making to encourage users to choose stronger and safer passwords. An imperative question relates to how users retort to goal-framed nudging that is intended to influence their actions associated with information security (Hong, 2012). Message framing has intermittently been recognized as a prime factor influencing user behavior (Rosoff *et al.*, 2013; Shropshire *et al.*, 2010). Similarly, contextual priming has been identified as a mechanism that can warn users of potential cybersecurity threats (Wright *et al.*, 2010). Digital nudging has been applied in a warning system to alert users to phishing emails (Cooper *et al.*, 2020).

2.2 User behavior in cybersecurity

Users are the weakest link or target toward cybersecurity-related threats (Siponen, 2000), and hence, more studies are needed to understand users' security responses and behavior (Lebek *et al.*, 2013). Self-efficacy has been shown to influence information security behavior (LaRose *et al.*, 2008). A survey study by Woon *et al.* (2005) has also demonstrated that perceived severity, response cost, perceived susceptibility and self-efficacy influence users' cybersecurity actions. Pahnila *et al.* (2007) found information quality of IS security policies to influence compliance. Their results also show that attitude, normative beliefs and habits have positive effects on intentions to comply with IS security policies, whereas threat appraisal and facilitating conditions have positive impact on attitude.

Efficacy of coping response positively influences behavioral intentions of users in implementing compliance behavior (Maddux and Rogers, 1983). Fear appeals can reduce cybersecurity threats by changing the security behavior of users in high-risk environments (Johnson and Warkentin, 2010). Although fear appeals are helpful in persuading users to comply with recommendations to mitigate cybersecurity risks, their effect is not consistent among users but is dependent on self-efficacy, response efficacy, threat severity and social influence (Johnson and Warkentin, 2010).

Several studies in IS security suggest that even though prior knowledge of risks is required to improve user security-related behavior, a multiplicity of other factors will also need to be examined along with the interaction effects of these factors (Lee and Kozar, 2005; Stanton *et al.*, 2005; Sasse *et al.*, 2001; Sharma, 2017). Organizational cybersecurity continues to be adversely affected by human errors associated with information security behavior.

2.3 Framing and priming in cybersecurity

Researchers have utilized prospect theory to evaluate the impact of positively versus negatively framed messages on user behavior (e.g. Aaker and Lee, 2001; Anderson and Agarwal, 2010; Pechmann *et al.*, 2003; Rodriguez-Priego *et al.*, 2020; Rosoff *et al.*, 2013; Sharma, 2017; Shiv *et al.*, 2004; Zhan *et al.*, 2020). In the cybersecurity context, Anderson and Agarwal (2010) found that users exhibit greater risk-averse behavior when presented with messages that focus on the benefits of following recommended secure online behaviors than the negative consequences of not following them. In contrast, an experimental study by Rodriguez-Priego *et al.* (2020) found that negative (loss) framing of security risks is more effective in influencing users toward taking more secure behavior than its positive (gain) framing counterpart. Another experimental study by Rosoff *et al.* (2013) did not find any difference in positive versus negative (gain-loss) framing of information security messages. Hence, the effect of positive versus negative framing on users' cybersecurity behavior is unclear or inconsistent in the literature.

Priming refers to a phenomenon, whereby the introduction of a stimulus affects how people respond to a subsequent stimulus (Weingarten *et al.*, 2016). Priming plays an important role in decision-making and can be presented as past instances along with their consequences. When past instances of experiences with security threats and their consequences are presented to users, they can change the users' information security behaviors. Safety-related priming has been shown to influence users' mobile app selection (Chong *et al.*, 2018). Priming in the form of a near-miss manipulation rather than as a purely negative event, which is the interest of this research, has resulted in users choosing safer actions. However, priming has been shown to be ineffective in preventing social engineering attacks to disclose personal information (Junger *et al.*, 2017).

3. Theoretical foundation and hypothesis development

In this section, we will review the dual-process theory, prospect theory and instance-based learning theory. These theories are then used to generate the research hypotheses.

3.1 Dual-process theory

The dual-process theory of controlled and automatic processing was first proposed by Shiffrin and Schneider (1977) and was later popularized by Kahneman (2011) in his book entitled "Thinking, Fast and Slow." In any decision-making context, we utilize one or two different information processing systems: (1) the automatic reactive system that is based on intuition or gut-feeling (system 1) where information processing is fast, emotional and unconscious and (2) the conscious cognitive system (system 2) where information processing is slow, controlled and deliberate. Our process of thinking or decision-making is conceptualized as an interaction between system 1 and system 2 (De Neys and Pennycook, 2019). System 1 uses automatic and effortless processing that typically occurs with routine tasks or familiar operations, whereas system 2 requires time and conscious effort to complete the task or activity. When using system 1, the decision can often be made in less than one second (Kahneman, 2011). In contrast, system 2 uses more time to generate a response or make a decision. Given that more than 90% of human decision-making utilizes system 1 thinking (Kahneman, 2011) and people tend to use system 1 when dealing with routine computer tasks, such as checking emails and opening websites, Goel *et al.* (2017) argued that social engineering attacks take place frequently because users are often using the automatic and nonconscious thinking process in system 1 when facing cybersecurity threats. Similarly, past research has raised concerns about the drawback of the automatic cognitive process of system 1 in responding to cybersecurity threats (Wang *et al.*, 2012). Social engineering attacks take advantage of people's tendency to pay more attention to visceral triggers (i.e. messages stressing the urgency of response) than to phishing deception indicators (i.e. errors or discrepancies in grammar, spelling or the sender's email address presented in a phishing email or message) (Wang *et al.*, 2012). Visceral triggers induce system 1 cognition which reduces information processing, whereas phishing deception indicators require system 2 cognition to recognize and process the deceptive nature and content. Because users tend to utilize system 1 thinking more than system 2 thinking, social engineering attacks are very common.

In principle, system 1 works continuously and creates judgments and assessments based on our past experiences and desires. During the decision-making process, system 1 runs automatically and systems 2 kicks in and gets activated when a new situation is encountered or if attention and conscious effort are required to complete the task at hand. Even when system 2 is activated, it tends to adopt the results of system 1 without modification, and hence, system 1 tends to have a strong impact on system 2.

Digital nudging can play an important role in information security decision-making by disrupting system 1 when the need arises. Nudging can be used to prompt users to reason through their choices in a more conscious and deliberate manner. However, it may also be used to prompt users to follow the default choice (e.g. click a link) that could be associated with a social engineering attack. In the latter case, digital nudging can reinforce the default option on the interface and facilitate system 1 thinking. Given that digital nudging has the potential to reinforce or disrupt the automatic reactive process of system 1, designers need to be mindful of the choices provided on an interface to either nudge the users to opt for a safe (i.e. risk-averse) action or disrupt system 1 thinking and trigger system 2's deliberation when users are facing potential cybersecurity threats. Digital nudging such as framing and priming can remind users about the potential consequences of such threats and thus, prompt them to carry out a careful and conscious thought process before selecting an appropriate choice. By utilizing system 2 thinking process, the degree of cybersecurity threats such as phishing can be minimized (Goel *et al.*, 2017).

3.2 Prospect theory

We draw upon the prospect theory to explain the effect of framing on user behavior (Tversky and Kahneman, 1986). Depending on the way information is presented, people can view message framing in cybersecurity communication as positive or negative. Framing can take one of two forms: (1) equivalence frames, where two logically equivalent options are presented in different ways or (2) emphasis frames, where two subsets of a situation are portrayed (Druckman, 2001). To comprehend decision-making, it is important to consider the kind of data or information (i.e. framing) that the user possesses or has access to in forming the basis of a decision (Sharma, 2017). In other words, both the data and the framing of the data can influence user judgments and decisions.

Prospect theory explains one's choices among alternatives that involve risk and uncertainty (Tversky and Kahneman, 1986; Lehto and Nah, 2006; Lehto *et al.*, 2012). The key concepts of prospect theory can be broken down into two phases. First, users make decisions by assessing the risks relative to a reference point (i.e. baseline) rather than based on the final consequence. The impact of this subjective assessment is known as framing, which refers to the way a prospect is subjectively estimated as either a gain or a loss, or whether a prospect is presented in a positive or negative way (Sharma, 2017). Hence, all the possible options are reformulated relative to the reference point to simplify the resulting evaluation (Tversky and Kahneman, 1984). With all the possible alternatives framed in a similar way, the user assesses each of the alternatives as either a gain or a loss and selects the one with the greatest valuation. Second, judgments are loss-aversive, which means that damages or losses are perceived as comparatively stronger than gains or benefits (Verendel, 2009).

The framing effect posits that the way options are displayed, such as whether options are presented as positively or negatively framed messages, affects individuals' responses to them (Plous, 1993). Individuals tend to avoid or stay away from threats when a positive message is displayed and identify or relate to the threats when a negative message is displayed (Tversky and Kahneman, 1984). Risk appraisal involves an assessment of the vulnerability of the threats (Rogers, 1975). Loss aversion in prospect theory posits that a loss is perceived to be more substantial than a gain of the same quantity. Messages that highlight the adverse consequences of an option are viewed as possible damages (losses) to which users are likely to react more strongly to as compared to messages that underline benefits (gains) (Tversky and Kahneman, 1984). Hence, negative framing is perceived as a loss of a greater magnitude than positive framing of the same magnitude.

3.3 Instance-based learning theory

We draw upon the instance-based learning theory to explain the effect of priming on user behavior (Gonzalez *et al.*, 2003). Instance-based learning theory explains how individuals make decisions based on their knowledge of similar instances. It suggests that when making decisions, individuals learn by accumulation, identification and refinement of instances or occurrences (Kanaparthi *et al.*, 2013).

According to instance-based learning theory, two cognitive factors, recency and inertia, impact users' learning and decision-making. Recency refers to relying on recent similar encounters to make choices, and inertia refers to using previous choices to make current choices. Based on instance-based learning theory, the first (acknowledgment) stage of decision-making involves scanning for choices to characterize relevant incidents. In the next (judgment) stage, knowledge or information is utilized to assess whether the present incident that is being assessed is seen as a risk or not. A decision is made among the choices based on inertia or recency recommended by the model (Gonzalez and Dutt, 2011).

When encountering an imminent risk, individuals evaluate the risk to determine the likelihood of the occurrence of the incident and the amount of damage that the incident could cause (Kaplan and Garrick, 1981). Prior knowledge or information about the incident is used to assess the risk (Fishbein and Ajzen, 2010; Krizan and Windschitl, 2007), where individuals recall related information from memory to carry out an assessment of the danger of the threat using the subjective expected utility model to decide on an action to take (Kahneman and Miller, 1986). Hence, information recall of related incidents plays an important role in influencing the action.

3.4 Hypotheses

This research will examine the impact of priming and framing of information security messages on users' behavior (i.e. action). The effect of priming will be hypothesized using the dual-process theory (Kahneman, 2011; Shiffrin and Schneider, 1977) and the instance-based learning theory (Gonzalez *et al.*, 2003; Gonzalez and Dutt, 2011). The effect of positive and negative framing will be hypothesized using the dual-process theory (Kahneman, 2011; Shiffrin and Schneider, 1977) and the prospect theory (Tversky and Kahneman, 1984, 1986).

Based on the dual-process theory, digital nudging in the form of priming (e.g. by posting specific past events or instances that remind users of a negative consequence) can disrupt or interrupt users' automatic processing of choices (system 1) associated with cybersecurity threats and nudged them to make a conscious effort in evaluating the choices presented to them (system 2). Based on instance-based learning theory, priming of past events that prompts users regarding potential harmful effects of available choices can create upsurge feelings of helplessness and drive individuals to opt for a safer option. When experiencing a similar encounter or instance to the primed message, the recognition process is activated due to the similarity of the primed instance and the instance that users are facing, resulting in users taking a deliberate and more cautious effort to evaluate their choices (system 2) in the context of the primed instance that highlights the unfavorable consequence of a previous event. As such, users are primed toward making a risk-averse decision. Hence, based on dual-process theory and instance-based learning theory, we hypothesize that:

H1. Priming users on cybersecurity risks reduces their risk-taking behavior associated with their cybersecurity action.

As mentioned earlier, the dual-process theory posits a dichotomy of two different systems of thinking in our cognitive system (Shiffrin and Schneider, 1977; Kahneman, 2011): System 1 (i.e. fast, automatic and instinctive way of making decisions) versus systems 2 (i.e. slow, deliberate and logical way of processing information to derive at a decision). Similar to the discussion earlier, digital nudging in the form of positive or negative framing can disrupt automatic processing (system 1) of choices presented to the users and spur a more deliberate and conscious effort to evaluate those choices (system 2). Thus, digital nudging in the form of negatively or positively framed messages works as the trigger to arouse system 2 from the automatic and default working of system 1. Hence, questions such as "What will happen if I open it?", "What will happen if I download it?", "Will I encounter a cyber-attack?" and "Do I need to be concerned about threats to my personal information privacy?" will be deliberated more carefully before a decision is reached. Hence, a "nudge" in the form of a positively or negatively framed message on cybersecurity threats is more likely to trigger the engagement of system 2 such that users reflect on and process the potential consequences of the choices given to them before making a decision. Hence, we propose that:

H2a. Providing users with negatively framed security messages reduces their risk-taking behavior associated with their cybersecurity action.

H2b. Providing users with positively framed security messages reduces their risk-taking behavior associated with their cybersecurity action.

The way in which information is presented or framed can influence decision-making (McDermott, 1991). Prospect theory can be used to explain the outcomes of framing. Decision-making based on prospect theory involves two phases. In the first phase, people assess the possible levels of risks involved in their given choices relative to a reference point (Tversky and Kahneman, 1984). In the second phase, each of these choices is assessed based on whether they are perceived as a gain or a loss. In line with prospect theory, decision-making in the second phase is loss aversive, which means people are more concerned about losses than gains and will react more strongly to negatively framed messages than positively framed messages. Hence, messages that highlight the adverse consequences of an option through negative framing are more likely to trigger risk-averse decisions as compared to similar messages framed positively. We, therefore, propose that:

H3. Negatively framed security messages will lead users to take a more risk-averse cybersecurity-related action than positively framed security messages.

4. Research methodology

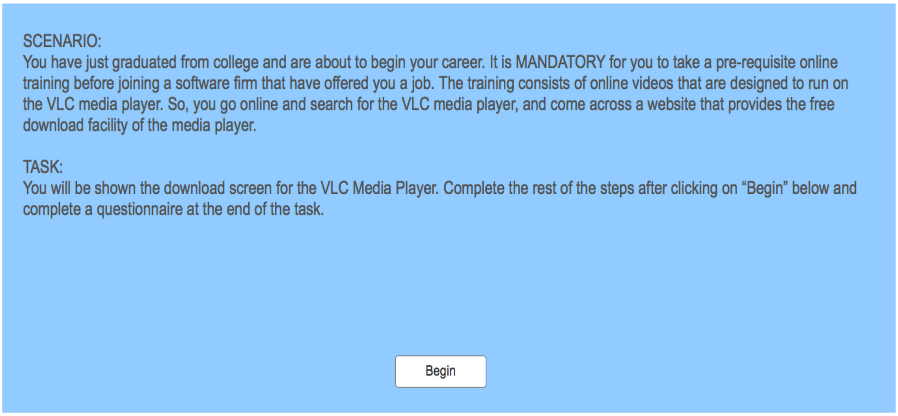
4.1 Experimental design

A 3 × 2 experimental study was conducted to test the hypotheses. The experiment consisted of three levels for framing (i.e. no framing, negative framing and positive framing) and two levels for priming (i.e. with and without priming). The no framing and no priming condition served as the control condition. Hence, participants were randomly assigned to one of the six experimental conditions: (1) no framing and no priming, (2) no framing with priming, (3) negative framing with no priming, (4) negative framing with priming, (5) positive framing with no priming and (6) positive framing with priming. They were provided with a cybersecurity online scenario that included the respective manipulation discussed above and were asked to make a decision between downloading or not downloading software.

4.2 Research task and procedures

This research study was conducted in a university's computer laboratory. The research task and procedures are described as follows: The cybersecurity scenario involved security threats related to downloading a media player from a site for online training purposes (see Figure 1). After clicking "Begin" (as shown in Figure 1), the download screen for a media player application was shown (see Figure 2). After clicking on "Download here", the next screen that appeared depends on the condition the participant was assigned to (see Appendix 1 for the snapshots of this screen). The operationalizations are further explained next.

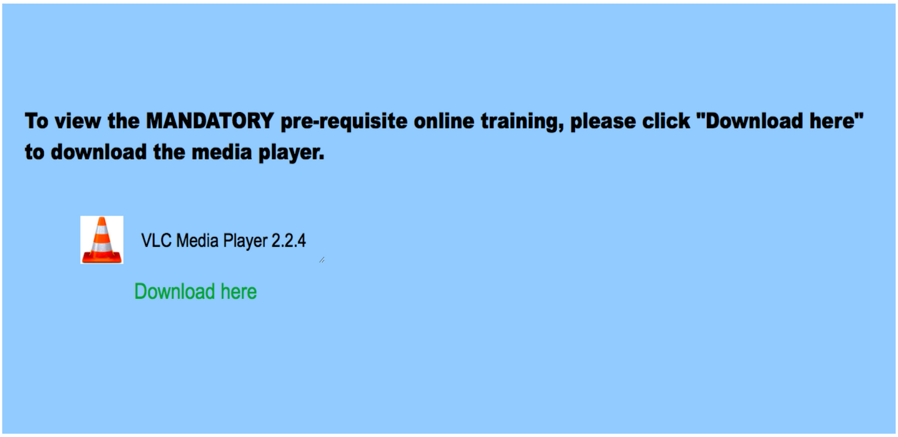
The negatively framed security messages emphasized the outcomes of not taking security safety measures and, accordingly, focused on the seriousness and likelihood of the dangers associated with the security threats. The positively framed security messages emphasized the advantages of executing security safeguards, for example, dependability, consistency and mental peace for both the users and their associations. Priming was operationalized by providing a user story about a similar security scenario containing the consequences of a known cybersecurity threat. The control condition did not display any security message (no framing) or user story (no priming).



SCENARIO:
You have just graduated from college and are about to begin your career. It is MANDATORY for you to take a pre-requisite online training before joining a software firm that have offered you a job. The training consists of online videos that are designed to run on the VLC media player. So, you go online and search for the VLC media player, and come across a website that provides the free download facility of the media player.

TASK:
You will be shown the download screen for the VLC Media Player. Complete the rest of the steps after clicking on "Begin" below and complete a questionnaire at the end of the task.

Figure 1.
Experiment scenario



To view the MANDATORY pre-requisite online training, please click "Download here" to download the media player.

Figure 2.
Download screen

The participants were asked to select one of two options: a safe (No – do not download) option or a risky (Yes – download) option, which serves as the dependent variable. This dependent variable, which we termed user action (or action for short), captured the outcomes of users' evaluation in dealing with the cybersecurity incident presented to them. After completing the cybersecurity online scenario by making a decision to download or not to download the media player, the participants completed a post-study questionnaire (see section 4.3 for more information).

In summary, each participant was provided with a negatively framed security message or a positively framed security message or no security message as well as presented with or without a user story depicting a prior cyber security-related incident. The scenarios presented to the participants were completely simulated by a software application, and hence, there was no real risk involved in the study.

Participants were provided with a consent form before the beginning of the study. The consent form indicated that their participation in the research study is voluntary. It also stated that they could choose not to participate or to withdraw their consent to participate at any time. The consent form indicated that they would not be penalized in any way should they decide not to participate or to withdraw from the study.

4.3 Measurement

The dependent variable for the study, Action, refers to the users' decision to download or not download the media player. After the participants have selected and indicated their action, a post-study questionnaire was used to capture the following five perceptions using the seven-point Likert scale (1 = strongly disagree to 7 = strongly agree): (1) *confidence with the action (or selection)*, (2) *perceived severity of the threat*, (3) *perceived susceptibility of the threat*, (4) *perceived trust in the download link* and (5) *fear associated with the action (or selection)*. The post-study questionnaire also included manipulation check questions to assess framing and priming. Appendix 2 presents the measurement items for the perceptual variables and the manipulation check questions.

We used four items to assess *confidence with action* (self-developed)*,* four items to assess *perceived severity of the threat* (adapted from Johnson and Warkentin, 2010), three items to assess *perceived susceptibility of the threat* (adapted from Johnson and Warkentin, 2010), three items to capture *trust associated with the download link* (adapted from Freed, 2014) and three items to assess *fear associated with the action* (adapted from Freed, 2014). *Confidence with action* was used to assess users' confidence in the action taken; *perceived severity of the threat* captured the perceived severity of the cyber threat associated with downloading the software; *perceived susceptibility of the threat* captured the perceived susceptibility of the cyber threat associated with downloading the software; *trust* captured trust in the download link and *fear* captured fear associated with the action taken.

We also captured the participants' demographic information, Internet usage, software download frequency and cybersecurity awareness. Appendix 3 shows these questionnaire items.

5. Results

The total number of participants in the study is 130. However, one participant experienced a computer crash in the middle of the experiment, and hence, 129 participants successfully completed the experiment. The final sample of 129 participants consisted of both male (65%) and female (35%) participants of which 93% of them were between 18–24 years old, 6% were between 25–34 years old and 1% were between 35–44 years old. The participants were students enrolled in technology-oriented business or information science and technology classes at a mid-western technological research university. The Internet usage, software download frequency and cybersecurity awareness of the participants are presented in

Table 1. As shown in Table 1, the participants are heavy or moderately heavy users of the Internet, where more than 80% of them have downloaded software at least once every few months and around 85% of them indicated that they are knowledgeable about phishing attacks. Hence, our sample is representative of tech-savvy young adults.

The framing manipulation check item (i.e. did the website provide a warning message that informed you about protecting your private information?) indicated a significant difference across the three framing conditions, i.e. no framing, positive framing and negative framing ($p = 0.002 < 0.05$). The priming manipulation check item (i.e. did the website provide a user story that assisted you in guiding your security action?) also showed a significant difference between priming and no priming conditions ($p = 0.001 < 0.05$).

The number of participants that was assigned to each of the conditions along with the number of participants that chose each option (safe or risky) is presented in Table 2.

Binary logistic regression is used for the data analysis because the dependent variable, action (i.e. safe or risky choice), is a binary variable that takes only two values (i.e. Yes [i.e. download – risky option] or No [i.e. do not download – safe option]). Binary logistic regression is used for analyzing the effects on a dichotomous dependent variable – as in this case where we are interested to assess whether the two independent variables, priming and framing, have an impact on the action taken by the users.

The results of the binary logistic regression are shown in Table 3. Because gender is insignificant when included as a covariate, we excluded it as a covariate in the data analysis. The parameter B is a logit coefficient that indicates the association between the independent

	Distribution (percentage)
Internet usage (hours per week)	
1–5	3.1%
6–10	12.4%
11–15	26.4%
16–20	20.9%
20+	37.2%
Software Download Frequency	
Once or more per week	13.9%
Two to three times per month	24.8%
Once per month	20.9%
Every few months	22.6%
Rarely or never	17.8%

Cybersecurity awareness questions	Percentage of “Yes” responses
Downloading and installing unlicensed software	50.4%
Use of common passwords across different settings	36.4%
Sharing passwords with others	38.8%
Knowledge of phishing attacks	84.5%

Table 1.
Internet usage, software download frequency and cybersecurity awareness of participants

	No priming			Priming		
	Safe option	Risky option	Total	Safe option	Risky option	Total
No framed message	5	16	21	12	9	21
Negative framing	10	12	22	15	7	22
Positive framing	10	11	21	11	11	22
Total	25	39	64	38	27	65

Table 2.
Descriptive statistics of download decisions

variables, framing and priming, and the dependent variable, action (Yes or No response to the download question). The standard error (S.E.) is used to compute the confidence interval, which is denoted as “C.I.” in Table 3. The Wald chi-square values and two-tailed p-values provide the results of hypothesis testing. The degree of freedom (df) is also provided. The odds ratio, Exp(B), signifies the strength of the association between two events or the possibility of a particular event happening with respect to the independent variables. Specifically, the odds ratio refers to the *odds* that an outcome will occur given a particular exposure compared to the *odds* of the outcome occurring in the absence of that exposure. Hence, a value of 1 signifies that there is no relationship.

As shown in Table 3, priming has a significant effect on the user action. In general, priming using a user story that depicts security threats is more likely to result in the safe action of not downloading the software ($B = 0.802$, Wald = 4.876, $p = 0.027 < 0.05$). Hence, hypothesis 1 is supported.

We compared the effect of providing a negatively framed message on cybersecurity threats versus the lack or absence of it. As shown in Table 3, the comparison of the negative framing condition and the control condition (no framing message) does not yield any significant difference ($B = 0.343$, Wald = 0.590, $p = 0.442$). Hence, hypothesis 2a is not supported. Similarly, a comparison of the positive framing condition versus the control condition (no framing message) also yields no significant difference ($B = 0.687$, Wald = 2.362, $p = 0.124$). Hence, hypothesis 2b is not supported.

As shown in Table 4, a comparison of the negative framed and positive framed conditions also yields no significant difference ($B = 0.321$; Wald: 0.555; $p = 0.456$). Hence, hypothesis 3 is also not supported.

In addition to analyzing H1, H2a, H2b and H3, we also captured user perceptions (see measurement items in Appendix 2) resulting from the experimental manipulations and the action taken by the user. All the measurement items loaded onto their target factors with loadings above 0.7 except item THSV4. Item THSV4 did not load well; hence, we ran the factor analysis again after dropping item THSV4. Table 5 presents the factor analysis results without item THSV4. As shown in Table 5, the measurement exhibits high convergent and discriminant validity, suggesting good construct validity (Cook and Campbell, 1979).

The Cronbach’s alpha coefficient (Cronbach, 1951) was used to assess the reliability of the measurement. The Cronbach’s alpha coefficients for all five factors are reported in Table 6,

							95% C.I. for EXP(B)	
	B	S.E.	Wald	df	Sig	Exp(B)	Lower	Upper
Framing			2.363	2	0.307			
Negative framing	0.343	0.447	0.590	1	0.442	1.409	0.587	3.383
Positive framing	0.687	0.447	2.362	1	0.124	1.987	0.828	4.770
Priming	0.802	0.363	4.876	1	0.027	2.229	1.094	4.542
Constant	−0.802	0.375	4.562	1	0.033	0.448		

Table 3. Results of binary logistic regression

							95% C.I. for EXP(B)	
	B	S.E.	Wald	df	Sig	Exp(B)	Lower	Upper
Framing	0.321	0.431	0.555	1	0.456	1.378	0.592	3.208
Constant	−0.047	0.305	0.023	1	0.879	0.955		

Table 4. Results of binary logistic regression for negative versus positive framing

Table 5.
Results of factor analysis (without item THSV4)

	Component				
	1	2	3	4	5
CONF4	*0.873*	−0.066	−0.035	−0.16	−0.136
CONF3	*0.843*	0.132	−0.03	−0.038	−0.148
CONF2	*0.84*	0.005	−0.003	−0.211	−0.208
CONF1	*0.757*	−0.059	0.156	−0.066	−0.234
TRUST2	−0.014	*0.929*	−0.042	0.093	0.048
TRUST1	0.038	*0.925*	−0.075	−0.009	0.065
TRUST3	−0.007	*0.92*	−0.105	0.058	0.022
THSV1	−0.063	−0.052	*0.898*	0.034	0.116
THSV2	0.028	0.013	*0.895*	−0.027	0.052
THSV3	0.112	−0.214	*0.847*	0.105	0.122
THSP3	−0.132	0.055	−0.021	*0.893*	0.153
THSP1	−0.093	0.02	0.003	*0.877*	0.165
THSP2	−0.221	0.088	0.165	*0.787*	0.324
FEAR2	−0.197	0.033	0.088	0.228	*0.842*
FEAR1	−0.295	0.021	0.1	0.179	*0.828*
FEAR3	−0.225	0.098	0.146	0.221	*0.787*

Note(s): Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization

Table 6.
Cronbach's alpha coefficients for perceptual variables

Construct	Cronbach's alpha coefficient
Confidence with action	0.88
Threat severity	0.87
Threat susceptibility	0.88
Trust	0.92
Fear	0.87

and they are all well above 0.7 (i.e. at least 0.87, as shown in Table 6). A value of 0.7 indicates adequate reliability (Nunnally *et al.*, 1967). Given that the Cronbach's alpha coefficients are 0.87 and higher, we conclude that the measurement items have high reliability and internal consistency.

As a secondary analysis, we examined the relationship between user decision (or action) and the perceptual variables – confidence with action, perceived severity, perceived susceptibility, trust and fear. The descriptive statistics are shown in Table 7.

We conducted multivariate ANOVA (MANOVA) to analyze whether the user download decision or action has significant effects on the perceptual variables. We found that gender is not a significant covariate and hence, excluded it from the analysis. The results of MANOVA are presented in Table 8. Based on the MANOVA results, confidence with action differed across action (i.e. choices made by the users) ($p < 0.01$). Participants who selected the safe option exhibited greater confidence associated with their action than participants who chose the risky option. Perceived severity ($p = 0.020 < 0.05$) and perceived susceptibility ($p = 0.016 < 0.05$) also differed across action. Hence, participants who chose the safe option (i.e. not to download the software) perceived greater severity and lower susceptibility associated with the cybersecurity threat than participants who chose to download the software. Moreover, we found a significant effect of trust across action ($p < 0.001$). Participants who chose not to download the software perceived lower trust in the download link than participants who chose to download the software. Interestingly, the level of fear did not differ across action ($p = 0.101$).

Table 7. Descriptive statistics of perceptual variables

	Action	*N*	Mean	Std. dev	Std. error mean
Confidence with action	Yes	66	5.133	1.093	0.135
	No	63	5.754	0.923	0.116
Perceived severity	Yes	66	5.05	1.359	0.167
	No	63	5.524	1.031	0.130
Perceived susceptibility	Yes	66	4.217	1.340	0.165
	No	63	3.567	1.636	0.206
Trust	Yes	66	4.429	1.275	0.157
	No	63	2.712	1.160	0.146
Fear	Yes	66	3.470	1.392	0.171
	No	63	3.085	1.446	0.182

Table 8. MANOVA results

Source		Type III sum of squares	df	Mean square	*F*	Sig
Action	Confidence with action	11.238	1	11.238	10.811	0.001
	Perceived severity	8.045	1	8.045	5.573	0.020
	Perceived susceptibility	13.393	1	13.393	6.015	0.016
	Trust	88.628	1	88.628	58.774	0.000
	Fear	5.456	1	5.456	2.728	0.101

6. Discussions of findings

We investigated the effect of framing and priming on users' cybersecurity behavior. Our study provides support that digital nudging in the form of priming can play an important role in the context of cybersecurity. The use of instance-based information to prime tech-savvy young adult users on potential security risks can lead them into taking safer security actions.

This research also explores the impact of positively and negatively framed security messages on users' behavior in the cybersecurity decision-making context. Drawing on prospect theory, we proposed that negatively framed messages could create fear sentiment by emphasizing the potential loss and hence, lead users to take safer security measures when compared to positively framed messages. However, our findings suggest that the framing of messages associated with cybersecurity risks does not have a significant effect on tech-savvy young adult users' behavior, or more specifically, their decision to download software or not. We believe that our framing of warning messages to users did not produce any effects because the warnings were generic and may not add any new information to the users. In other words, our operationalization of positive framing was presented in the form of reminders to users that their information would be protected by choosing not to download the software, which may not be surprising to the participants. Given that our participants are tech-savvy, the operationalization of negative framing in the form of warnings about exposure of private information may also not be surprising to them. It is also possible that the warning messages in the study were not framed strongly enough.

A secondary analysis was conducted to assess whether user perceptions measured after the action was selected differed across users who took different actions. The findings suggest that confidence with action, perceived severity, perceived susceptibility and trust differed across users who selected different actions, but fear appeals did not differ. Participants who had taken a risk-averse cybersecurity action showed greater confidence associated with their action, perceived greater severity associated with cybersecurity risks, perceived lower susceptibility to cybersecurity risks and perceived lower trust in the download link.

We also believe that a difference in fear appeals was not observed because there was no stake for the participants in this simulated study.

7. Conclusions and implications

Digital nudging can play an important role in reducing users' exposure to cybersecurity threats. In the context of this research, instance-based priming can nudge tech-savvy young adult users into taking risk-averse actions, but positive and negative framing of the available choices does not seem to influence their choices. Our study has implications for theory, practice and future studies.

We have demonstrated that instance-based learning theory can be applied in priming users toward taking risk-averse actions associated with cybersecurity threats. By using similar instances of cybersecurity threats for priming, it is easier for users to relate directly to the instance presented and evaluate the risks of the cybersecurity threat that they face. Hence, this research provides a theory-driven understanding of how information security messages in the form of priming can lead to safer cybersecurity actions.

Our findings show that digital nudging in the IS literature can be applied and generalized to the information security context. Weinmann *et al.* (2016) defined the term "digital nudging" and believe that it is an effective way to influence people's decisions by changing their decision environment, or more specifically, by modifying or making minor changes to the interface. Our study suggests that tech-savvy young adult users are less likely to engage in risky cybersecurity actions when they are primed using similar instances regarding security risks. In other words, digital nudging in the form of priming could reduce exposure to cybersecurity risks. Designers of information systems and security systems can use these results to make subtle design changes to their interface. Priming users with similar instances of cybersecurity attacks can increase their risk-averse behavior. We hope that designers can introduce instance-based priming in the applications they develop.

Our study also has implications for future research on the framing effect of security warning messages. We draw on the prospect theory to understand whether negatively framed messages would lead users to take safe security measures as compared to positively framed messages. Our findings suggest that positive and negative framing has no effect on user behavior. The results are not consistent with some of the existing literature. Future research can replicate this study and explore different types of framing manipulations in the information security context.

This study was conducted in a university lab using lab computers. Future studies can overcome this limitation by having participants use their laptops. In this way, it is possible to analyze whether participants would respond differently while encountering a security threat on their personal computers versus public computers or work computers.

The participants of the study were students enrolled in technology-oriented business or information science and technology classes at a mid-western technological research university. Replications of this study can be carried out to extend its generalizability or external validity. In future research, we could carry out this research as an online field experiment (e.g. through crowdsourcing sites such as Mechanical Turk or online panels/communities) to reach out to a more diverse sample that is more representative of the US population.

More research is warranted to reduce the vulnerability of users to cybersecurity threats. In this research, we found that instance-based priming can increase risk-averse decisions or decrease risk-taking behavior of tech-savvy young adults. However, we did not find any effect of framing of information security messages on decisions or actions involving cybersecurity threats. Some possible reasons for not finding any framing effect could be due to the lack of new information presented in the message (due to familiarity with standard download choices and expected consequences) or the lack of stake in decision-making in the simulated study. Future research can examine framing of unfamiliar rather than familiar choices and/or introducing a stake or penalty as part of the study.

Finally, framing should be studied from multiple perspectives. Levin *et al.* (1998) conceptualized three types of framing, goal framing, attribute framing and risky choice framing. Our study focuses on goal framing and emphasizes decisions to download or not download software. Goal framing refers to nudging users by emphasizing either the goal of obtaining the positive consequence (i.e. gain) or avoiding the negative consequence (i.e. loss). Attribute framing refers to framing the same attribute in multiple ways. Risky choice framing involves nudging users toward a specific choice. Framing needs to be studied in a variety of cybersecurity contexts to gain a complete understanding of its impact and effectiveness in influencing user decision-making and behavior. Hence, future research should study all three types of framing to fully understand the effects of framing on cybersecurity behaviors.

References

Aaker, J.L. and Lee, A.Y. (2001), "'I' seek pleasures and 'we' avoid pains: the role of self-regulatory goals in information processing and persuasion", *Journal of Consumer Research*, Vol. 28 No. 1, pp. 33-49.

Akhawe, D. and Felt, A.P. (2013), "Alice in warningland: a large-scale field study of browser security warning effectiveness", *22nd {USENIX} Security Symposium ({USENIX} Security 13)*, pp. 257-272.

Anderson, C.L. and Agarwal, R. (2010), "Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions", *MIS Quarterly*, Vol. 24 No. 3, pp. 613-643.

Bernard, T.S. and Cowley, S. (2017), "Equifax breach caused by lone employee's error, former C.E.O. says", *The New York Times*, Vol. 3 October, available at: https://www.nytimes.com/2017/10/03/business/equifax-congress-data-breach.html.

Carpenter, P. (2020), "Beware of these top five social engineering scams", *Forbes*, Vol. 26 October, available at: https://www.forbes.com/sites/forbesbusinesscouncil/2020/10/26/beware-of-these-top-five-social-engineering-scams/.

Castleman, B.L. and Page, L.C. (2016), "Freshman year financial aid nudges: an experiment to increase FAFSA renewal and college persistence", *Journal of Human Resources*, Vol. 51 No. 2, pp. 389-415.

Chen, J., Gates, C.S., Li, N. and Proctor, R.W. (2015), "Influence of risk/safety information framing on android app-installation decisions", *Journal of Cognitive Engineering and Decision Making*, Vol. 9 No. 2, pp. 149-168.

Chong, I., Ge, H., Li, N. and Proctor, R.W. (2018), "Influence of privacy priming and security framing on mobile app selection", *Computers and Security*, Vol. 78, pp. 143-154.

Cook, T.D. and Campbell, D.T. (1979), *Quasi-experimentation: Design and Analysis Issues for Field Settings*, Houghton Mifflin, Boston, Massachusetts, MA.

Cooper, M., Levy, Y., Wang, L. and Dringus, L. (2020), "Subject matter experts' feedback on a prototype development of an audio, visual, and haptic phishing email alert system", *Online Journal of Applied Knowledge Management*, Vol. 8 No. 2, pp. 107-121.

Cronbach, L.J. (1951), "Coefficient alpha and the internal structure of tests", *Psychometrika*, Vol. 16 No. 3, pp. 297-334.

Damgaard, M.T. and Nielsen, H.S. (2018), "Nudging in education", *Economics of Education Review*, Vol. 64, pp. 313-342.

De Neys, W. and Pennycook, G. (2019), "Logic, fast and slow: advances in dual-process theorizing", *Current Directions in Psychological Science*, Vol. 28 No. 5, pp. 503-509.

Dennis, A.R., Yuan, L., Feng, X., Webb, E. and Hsieh, C.J. (2020), "Digital nudging: numeric and semantic priming in e-commerce", *Journal of Management Information Systems*, Vol. 37 No. 1, pp. 39-65.

Druckman, J.N. (2001), "The implications of framing effects for citizen competence", *Political Behavior*, Vol. 23 No. 3, pp. 225-256.

Dubov, A. and Phung, C. (2015), "Nudges or mandates? The ethics of mandatory flu vaccination", *Vaccine*, Vol. 33 No. 22, pp. 2530-2535.

Fishbein, M. and Ajzen, I. (2010), *Predicting and Changing Behavior: the Reasoned Action Approach*, Psychology Press, New York, NY.

Freed, S.E. (2014), *Examination of Personality Characteristics Among Cybersecurity and Information Technology Professionals*, Unpublished Master Thesis, University of Tennessee at Chattanooga.

Goel, S., Dennis, A., Williams, K. and Babb, J. (2017), "A proposal to reconsider learned security behaviors to improve user response to phishing emails", *Proceedings of the 2017 IFIP 8.11/ 11.13 Dewald Roode Information Security Research Workshop*, 6–7 October, Tampa, FL, available at: https://ifip.byu.edu/2017/Goel_2017.pdf.

Gonzalez, C. and Dutt, V. (2011), "Instance-based learning: integrating decisions from experience in sampling and repeated choice paradigms", *Psychological Review*, Vol. 118 No. 4, pp. 523-551.

Gonzalez, C., Lerch, J.F. and Lebiere, C. (2003), "Instance-based learning in dynamic decision making", *Cognitive Science*, Vol. 27 No. 4, pp. 591-635.

Halevi, T., Lewis, J. and Memon, N. (2013), "A pilot study of cyber security and privacy related behavior and personality traits", *Proceedings of the 22nd International Conference on World Wide Web*, pp. 737-744.

Hong, J. (2012), "The state of phishing attacks", *Communications of the ACM*, Vol. 55 No. 1, pp. 74-81.

IBM Corporation (2014), "IBM security services 2014 cyber security intelligence index", available at: https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF.

Johnston, A.C. and Warkentin, M. (2010), "Fear appeals and information security behaviors: an empirical study", *MIS Quarterly*, Vol. 34 No. 3, pp. 549-566.

Junger, M., Montoya, L. and Overink, F.J. (2017), "Priming and warnings are not effective to prevent social engineering attacks", *Computers in Human Behavior*, Vol. 66, pp. 75-87.

Kahneman, D. (2011), *Thinking, Fast and Slow*, Farrar, Straus and Giroux, New York, NY.

Kahneman, D. and Miller, D.T. (1986), "Norm theory: comparing reality to its alternatives", *Psychological Review*, Vol. 93 No. 2, pp. 136-153.

Kanaparthi, B., Reddy, R. and Dutt, V. (2013), "Cyber situation awareness: rational methods versus instance-based learning theory for cyber threat detection", *Proceedings of the12th International Conference on Cognitive Modeling*. Ottawa, ON, Canada.

Kaplan, S. and Garrick, B.J. (1981), "On the quantitative definition of risk", *Risk Analysis*, Vol. 1 No. 1, pp. 11-27.

Krishna, A., Wagner, M., Yoon, C. and Adaval, R. (2006), "Effects of extreme-priced products on consumer reservation prices", *Journal of Consumer Psychology*, Vol. 16 No. 2, pp. 176-190.

Krizan, Z. and Windschitl, P.D. (2007), "The influence of outcome desirability on optimism", *Psychological Bulletin*, Vol. 133 No. 1, pp. 95-121.

LaRose, R., Rifon, N.J. and Enbody, R. (2008), "Promoting personal responsibility for Internet safety", *Communications of the ACM*, Vol. 51 No. 3, pp. 71-76.

Lebek, B., Uffen, J., Breitner, M.H., Neumann, M. and Hohler, B. (2013), "Employees' information security awareness and behavior: a literature review", *Proceedings of the 46th Hawaii International Conference on System Sciences*, IEEE Computer Society, Wailea, HI, pp. 2978-2987.

Lee, Y. and Kozar, K.A. (2005), "Investigating factors affecting the adoption of anti-spyware systems", *Communications of the ACM*, Vol. 48 No. 8, pp. 72-77.

Lehto, M.R. and Nah, F. (2006), "Decision-making models and decision support", in Salvendy, G. (Ed.), *Handbook of Human Factors and Ergonomics*, 3rd ed., John Wiley & Sons, Hoboken, New Jerssey, NJ, pp. 191-242.

Lehto, M.R., Nah, F. and Yi, J.S. (2012), "Decision-making models, decision support, and problem solving", in Salvendy, G. (Ed.), *Handbook of Human Factors and Ergonomics*, 4th ed., John Wiley & Sons, Hoboken, New Jerssey, NJ, pp. 192-242.

Levin, I.P., Schneider, S.L. and Gaeth, G.J. (1998), "All frames are not created equal: a typology and critical analysis of framing effects", *Organizational Behavior and Human Decision Processes*, Vol. 76 No. 2, pp. 149-188.

Maddux, J.E. and Rogers, R.W. (1983), "Protection motivation and self-efficacy: a revised theory of fear appeals and attitude change", *Journal of Experimental Social Psychology*, Vol. 19 No. 5, pp. 469-479.

Marx, B.M. and Turner, L.J. (2019), "Student loan nudges: experimental evidence on borrowing and educational attainment", *American Economic Journal: Economic Policy*, Vol. 11 No. 2, pp. 108-141.

McDermott, L.C. (1991), "Millikan lecture 1990: what we teach and what is learned—closing the gap", *American Journal of Physics*, Vol. 59 No. 4, pp. 301-315.

McNeese, M., Cooke, N.J., D'Amico, A., Endsley, M.R., Gonzalez, C., Roth, E. and Salas, E. (2012), "Perspectives on the role of cognition in cyber security", *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 56 No. 1, pp. 268-271.

Nunnally, J.C., Bernstein, I.H. and Berge, J.M. (1967), *Psychometric Theory*, McGraw-Hill, New York, NY.

Pahnila, S., Siponen, M. and Mahmood, A. (2007), "Employees' behavior toward IS security policy compliance", *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*. IEEE Computer Society, Waikoloa, Big Island, HI, USA.

Pechmann, C., Zhao, G., Goldberg, M. and Reibling, E. (2003), "What to convey in antismoking advertisements for adolescents: the use of protection motivation theory to identify effective message themes", *Journal of Marketing*, Vol. 67 No. 2, pp. 1-18.

Peer, E., Egelman, S., Harbach, M., Malkin, N., Mathur, A. and Frik, A. (2020), "Nudge me right: personalizing online security nudges to people's decision-making styles", *Computers in Human Behavior*, Vol. 109, 106347.

Plous, S. (1993), *The Psychology of Judgment and Decision Making*, McGraw-Hill, New York, NY.

Renaud, K. and Zimmermann, V. (2018), "Guidelines for ethical nudging in password authentication", *SAIEE Africa Research Journal*, Vol. 109 No. 2, pp. 102-118.

Rodriguez-Priego, N., van Bavel, R., Vila, J. and Briggs, P. (2020), "Framing effects on online security behavior", *Frontiers in Psychology*, Vol. 11, 527886.

Rogers, R.W. (1975), "A protection motivation theory of fear appeals and attitude change", *The Journal of Psychology*, Vol. 91 No. 1, pp. 93-114.

Rosoff, H., Cui, J. and John, R.S. (2013), "Heuristics and biases in cyber security dilemmas", *Environment Systems and Decisions*, Vol. 33 No. 4, pp. 517-529.

Sasse, M.A., Brostoff, S. and Weirich, D. (2001), "Transforming the 'weakest link'—a human/computer interaction approach to useable and effective security", *BT Technology Journal*, Vol. 19 No. 3, pp. 122-131.

Schneider, C., Weinmann, M. and vom Brocke, J. (2018), "Digital nudging–influencing choices by using interface design", *Communications of the ACM*, Vol. 61 No. 7, pp. 67-73.

Sharma, K. (2017), *Impact of Framing and Priming on Users' Behavior in Cybersecurity*, Unpublished master's thesis, Missouri University of Science and Technology, Rolla, MO.

Shiffrin, R.M. and Schneider, W. (1977), "Controlled and automatic human information processing: II. Perceptual learning, automatic attending and a general theory", *Psychological Review*, Vol. 84, pp. 127-190.

Shiv, B., Edell, J. and Payne, J.W. (2004), "Does elaboration increase or decrease the effectiveness of negatively versus positively framed messages", *Journal of Consumer Research*, Vol. 31 No. 1, pp. 199-208.

Shropshire, J.D., Warkentin, M. and Johnston, A.C. (2010), "Impact of negative message framing on security adoption", *Journal of Computer Information Systems*, Vol. 51 No. 1, pp. 41-51.

Shropshire, J., Warkentin, M. and Sharma, S. (2015), "Personality, attitudes, and intentions: predicting initial adoption of information security behavior", *Computers and Security*, Vol. 49, pp. 177-191.

Siponen, M.T. (2000), "Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice", *Information Management and Computer Security*, Vol. 8 No. 5, pp. 197-209.

Smith, S.N., Nah, F.F.H. and Cheng, M.X. (2016), "The impact of security cues on user perceived security in e-commerce", in Tryfonas, T. (Ed.), *Lecture Notes in Computer Science 9750*, Springer, Cham, pp. 164-173.

Stanton, J., Mastrangelo, P.R., Stam, K.R. and Jolton, J. (2004), "Behavioral information security: two end user survey studies of motivation and security practices", *Proceedings of the Tenth Americas Conference on Information Systems*, New York, NY.

Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. (2005), "Analysis of end user security behaviors", *Computers and Security*, Vol. 24 No. 2, pp. 124-133.

Stephanidis, C., Salvendy, G., Antona, M., Chen, J.Y.C., Dong, J., Duffy, V.G., Fang, X., Fidopiastis, C., Fragomeni, G., Fu, L.P., Guo, Y., Harris, D., Ioannou, A., Jeong, K., Konomi, S., Krömker, H., Kurosu, M., Lewis, J.R., Marcus, A., Meiselwitz, G., Moallem, A., Mori, H., Nah, F., Ntoa, S., Rau, P.P., Schmorrow, D., Siau, K., Streitz, N., Wang, W., Yamamoto, S., Zaphiris, P. and Zhou, J. (2019), "Seven HCI grand challenges", *International Journal of Human-Computer Interaction*, Vol. 35 No. 14, pp. 1229-1269.

Thaler, R.H. and Sunstein, C.R. (2009), *Nudge: Improving Decisions about Health, Wealth, and Happiness*, Penguin Books, London, available at: https://www.amazon.com/Nudge-Improving-Decisions-Health-Happiness/dp/014311526X.

Thibodeaux, B (2021), "Five cyber threats to watch in 2021", *Security*, available at: https://www.securitymagazine.com/articles/94343-five-cyber-threats-to-watch-in-2021.

Tversky, A. and Kahneman, D. (1984), "Choice, values and frames", *American Psychologist*, Vol. 39 No. 4, pp. 341-350.

Tversky, A. and Kahneman, D. (1986), "Rational choice and the framing of decisions", *The Journal of Business*, Vol. 59 No. 4, pp. S251-S278.

Verendel, V. (2009), "Quantified security is a weak hypothesis: a critical survey of results and assumptions", *Proceedings of the 2009 Workshop on New Security Paradigms*, pp. 37-50.

Wang, J., Herath, T., Chen, R., Vishwanath, A. and Rao, H.R. (2012), "Research article phishing susceptibility: an investigation into the processing of a targeted spear phishing email", *IEEE Transactions on Professional Communication*, Vol. 55 No. 4, pp. 345-362.

Wang, J., Shan, Z., Gupta, M. and Rao, H.R. (2019), "A longitudinal study of unauthorized access attempts on information systems: the role of opportunity contexts", *MIS Quarterly*, Vol. 43 No. 2, pp. 601-622.

Weingarten, E., Chen, Q., McAdams, M., Yi, J., Hepler, J. and Albarracín, D. (2016), "From primed concepts to action: a meta-analysis of the behavioral effects of incidentally presented words", *Psychological Bulletin*, Vol. 142 No. 5, pp. 472-497.

Weinmann, M., Schneider, C. and vom Brocke, J. (2016), "Digital nudging", *Business and Information Systems Engineering*, Vol. 58 No. 6, pp. 433-436.

Woon, I., Tan, G.-W. and Low, R.T. (2005), “A protection motivation theory approach to home wireless security”, *Proceedings of the 26th International Conference on Information Systems*, pp. 367-380.

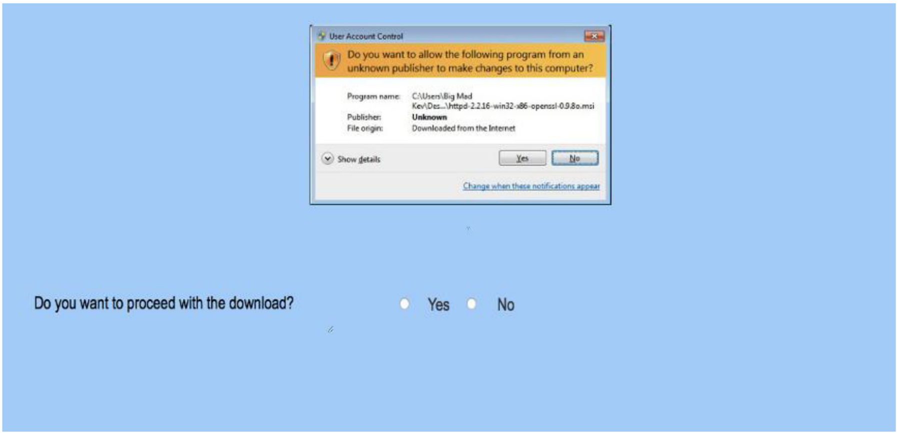
Wright, R., Chakraborty, S., Basoglu, A. and Marett, K. (2010), “Where did they go right? Understanding the deception in phishing communications”, *Group Decision and Negotiation*, Vol. 19, pp. 391-416.

Yakencheck, J. (2019), “Lessons of the capital one data breach”, *InfoSecurity*, available at: https://www.infosecurity-magazine.com/infosec/lessons-from-the-capital-one-data/.

Zhan, X., Nah, F., Siau, K., Hall, R. and Cheng, M. (2020), “Presentation of computer security risk information: impact of framing and base size”, *Proceedings of the 2020 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop, (conducted virtually)*, Ames, Iowa, available at: https://ifip.byu.edu/2020/DRW2020_paper_9.pdf.

Appendix 1
Snapshots of experimental conditions

(1) Control condition (no framed message and no priming)

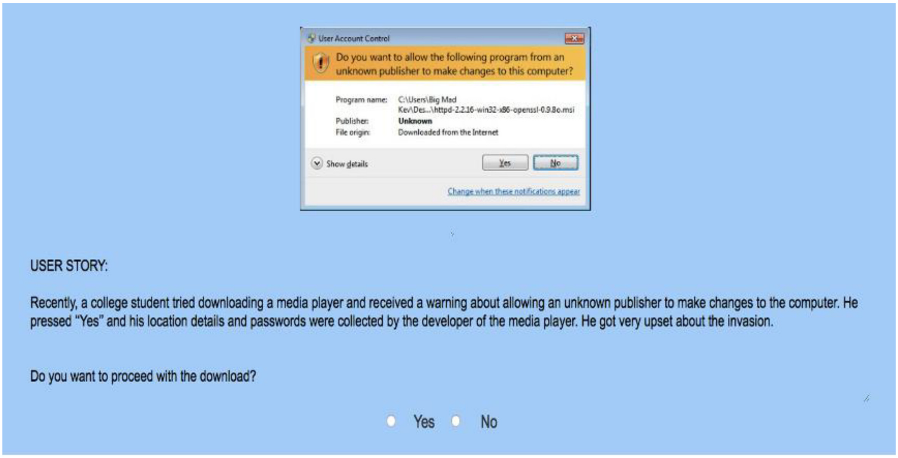


Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: C:\Users\Big Mad Kev\Des...\httpd-2.2.16-win32-x86-openssl-0.9.8o.msi
Publisher: **Unknown**
File origin: Downloaded from the Internet

Do you want to proceed with the download? ○ Yes ○ No

(2) No framed message and priming



Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: C:\Users\Big Mad Kev\Des...\httpd-2.2.16-win32-x86-openssl-0.9.8o.msi
Publisher: **Unknown**
File origin: Downloaded from the Internet

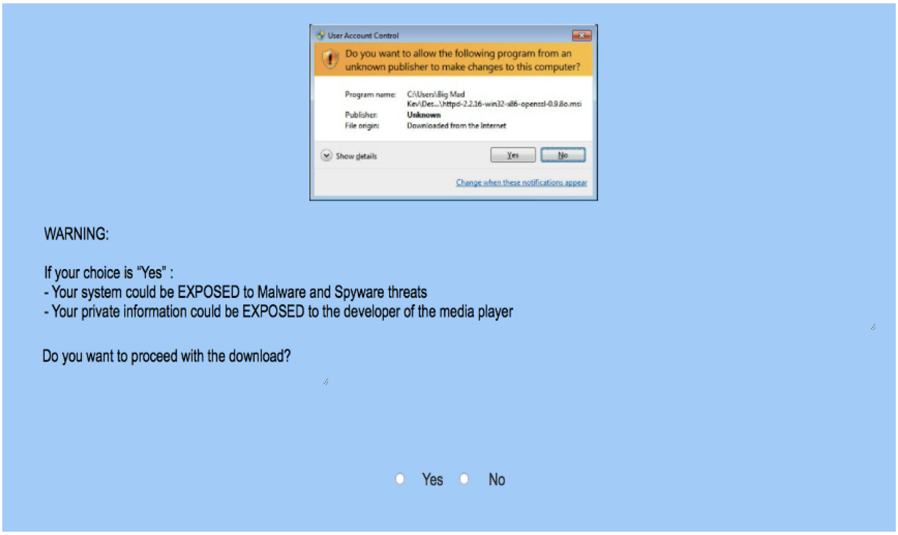
USER STORY:

Recently, a college student tried downloading a media player and received a warning about allowing an unknown publisher to make changes to the computer. He pressed "Yes" and his location details and passwords were collected by the developer of the media player. He got very upset about the invasion.

Do you want to proceed with the download?

○ Yes ○ No

(3) Negative framing with no priming


User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: C:\Users\Big Mad Kev\Des...\httpd-2.2.16-win32-x86-openssl-0.9.8o.msi
Publisher: **Unknown**
File origin: Downloaded from the Internet

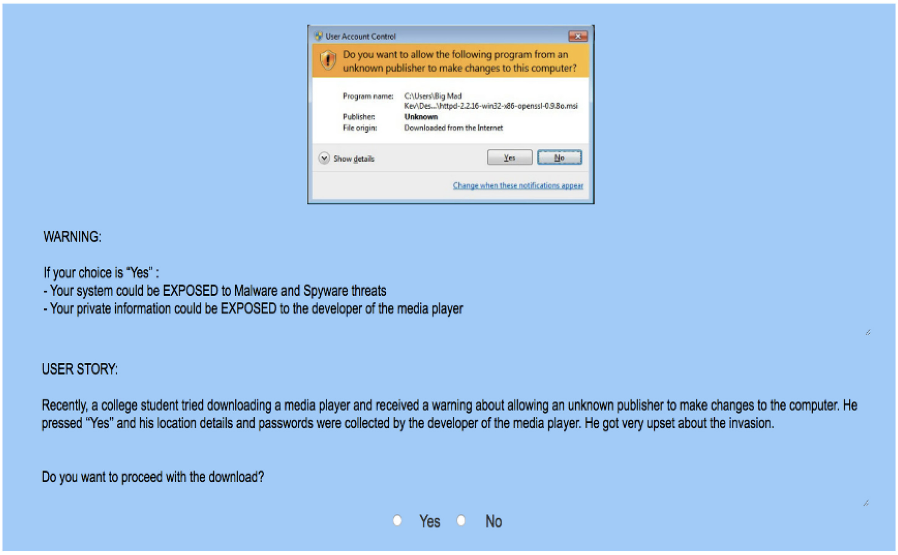
WARNING:

If your choice is "Yes" :
- Your system could be EXPOSED to Malware and Spyware threats
- Your private information could be EXPOSED to the developer of the media player

Do you want to proceed with the download?

○ Yes ○ No

(4) Negative framing with priming


User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: C:\Users\Big Mad Kev\Des...\httpd-2.2.16-win32-x86-openssl-0.9.8o.msi
Publisher: **Unknown**
File origin: Downloaded from the Internet

WARNING:

If your choice is "Yes" :
- Your system could be EXPOSED to Malware and Spyware threats
- Your private information could be EXPOSED to the developer of the media player

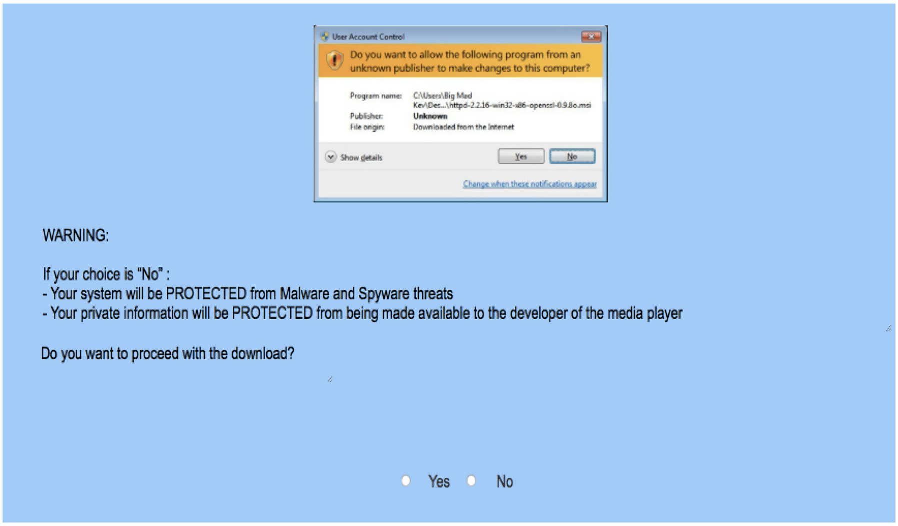
USER STORY:

Recently, a college student tried downloading a media player and received a warning about allowing an unknown publisher to make changes to the computer. He pressed "Yes" and his location details and passwords were collected by the developer of the media player. He got very upset about the invasion.

Do you want to proceed with the download?

○ Yes ○ No

(5) Positive framing with no priming



User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: C:\Users\Big Mad Kev\Des...\httpd-2.2.16-win32-x86-openssl-0.9.8o.msi
Publisher: Unknown
File origin: Downloaded from the Internet

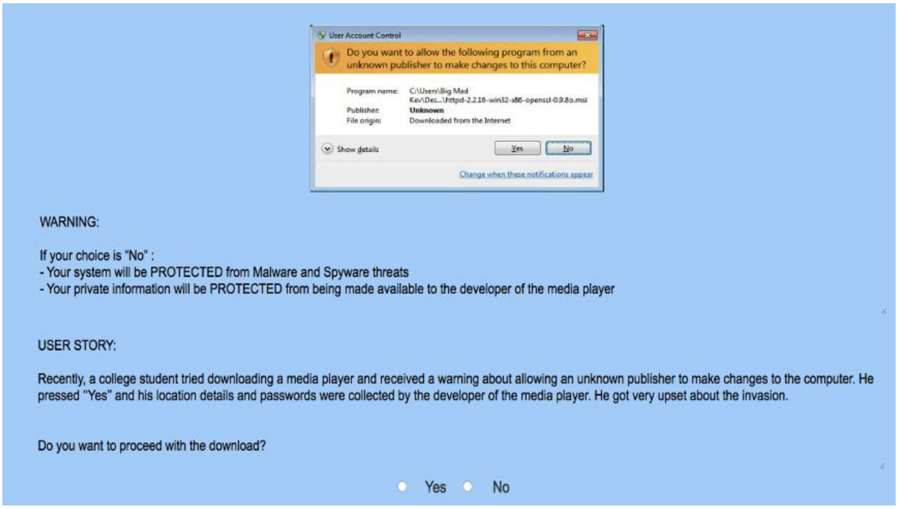
WARNING:

If your choice is "No" :
- Your system will be PROTECTED from Malware and Spyware threats
- Your private information will be PROTECTED from being made available to the developer of the media player

Do you want to proceed with the download?

○ Yes ○ No

(6) Positive framing with priming



User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: C:\Users\Big Mad Kev\Des...\httpd-2.2.16-win32-x86-openssl-0.9.8o.msi
Publisher: Unknown
File origin: Downloaded from the Internet

WARNING:

If your choice is "No" :
- Your system will be PROTECTED from Malware and Spyware threats
- Your private information will be PROTECTED from being made available to the developer of the media player

USER STORY:

Recently, a college student tried downloading a media player and received a warning about allowing an unknown publisher to make changes to the computer. He pressed "Yes" and his location details and passwords were collected by the developer of the media player. He got very upset about the invasion.

Do you want to proceed with the download?

○ Yes ○ No

Appendix 2
Measurement items and manipulation checks

	Measurement items (7-point Likert scale)
Confidence with action (developed by the authors)	(CONF1) I am confident about the action I took
	(CONF2) I would choose the same action again
	(CONF3) I believe I had taken the right action
	(CONF4) I am confident about my action
Perceived severity (Johnston and Warkentin, 2010)	(THSV1) If malware would infect my computer, it would be severe
	(THSV2) If malware would infect my computer, it would be serious
	(THSV3) If malware would infect my computer, it would be significant
	(THSV4) Having my identity stolen is a serious problem for me
Perceived susceptibility (Johnston and Warkentin, 2010)	(THSP1) My computer is at risk of becoming infected with malware
	(THSP2) It is likely that my computer has been infected with malware
	(THSP3) It is possible that my computer has been infected with malware
Trust (Freed, 2014)	(TRUST1) I believe that the download link is trustworthy
	(TRUST2) I trust the vendor of the download link
	(TRUST3) I trust the download link
Fear (Freed, 2014)	(FEAR1) I was worried about the action I took
	(FEAR2) I was concerned about the action I took
	(FEAR3) I experienced fear in the action I took
	Measurement items (Yes/No scale)
Framing (developed by the authors)	(FRM) Did the website provide a warning message that informed you about *protecting* your private information?
Priming (developed by the authors)	(PRM) Did the website provide a *user story* that assisted you in guiding your security action?

Appendix 3
Questionnaire on demographics, Internet usage, software download frequency and cybersecurity awareness

(1) Gender - What is your gender? (Male, Female)

(2) Age - How old are you? (18–24, 25–34, 35–44, 45–54, 55–64, 65–74 and, 75 or older)

(3) Online Internet usage - Approximately how many hours do you spend online per week? (1–5, 6–10, 11–15, 16–20, 20+)

(4) Software download frequency - Approximately how often do you download software from the Internet? (Once or more per month, two to three times per month, once per month, every few months, rarely or never)

(5) Cybersecurity awareness - Do you download and install unlicensed software? (Yes, No)

(6) Cybersecurity awareness - Do you use the same passwords for your school accounts as you do for your personal accounts at home, such as Facebook, Twitter or your personal email accounts? (Yes, No)

(7) Cybersecurity awareness - Have you ever shared your passwords with others? (Yes, No)

(8) Cybersecurity awareness - Do you know what a phishing attack is? (Yes, No)

Corresponding author

Fiona Fui-Hoon Nah can be contacted at: fiona.nah@cityu.edu.hk