



Device and risk-avoidance behavior in the context of cybersecurity phishing attacks

Naama Ilany-Tzur^{a,*}, Lior Fink^b

^a Carnegie Mellon University, Pittsburgh, PA, USA

^b Ben-Gurion University of the Negev, Beer-Sheva, Israel

ARTICLE INFO

Keywords:

Mobile use

Cybersecurity

Risk-avoidance behavior

Technology threat avoidance theory (TTAT)

ABSTRACT

Phishing has been the most common type of cybercrime in recent years. The fact that successful phishing attempts require victims to collaborate with their attackers highlights the importance of identifying factors that influence users' avoidance behavior. Drawing from evidence that mobile users process information differently than personal computer (PC) users, this research suggests that the device used may influence users' risk-avoidance behavior, as manifested in their tendency to avoid clicking on potentially risky messages. Indeed, three studies suggest that mobile users are more risk-avoidant than PC users. Specifically, analyzing data from a cybersecurity company regarding ~500,000 URL requests in a sample of household networks, we show that mobile devices are less likely than PCs to access unsafe URLs. Next, in two online controlled experiments in which device and URL risk levels were randomly assigned, we show that mobile users are less likely than PC users to click on a URL in a phishing-like message. Notably, this difference is observed for lower-risk URLs, whereas PC and mobile users display similar risk-avoidance tendencies in the presence of highly risky URLs. This work contributes to the mobile use literature, as well as to developing information systems theory regarding technology-threat avoidance, by showing that the device used is a contextual factor influencing users' susceptibility to phishing attacks.

1. Introduction

According to the 2024 FBI Internet Crime Report, the total number of reported internet crimes that year reached a record number of 859,532 complaints (FBI Internet Crime Report 2025). This increase continues a trend that has accelerated in recent years. According to this report, estimated losses due to internet crimes reached a record of 16.6 billion US dollars, which is 33 % higher than the estimated losses in 2023. Phishing was the most common type of cybercrime in 2024, and the number of phishing incidents (193,407) was more than double the number of the second most common type of incidents (FBI Internet Crime Report, 2025).

Phishing is a form of online fraud in which an attacker, masquerading as a trusted entity (e.g., a financial institution), dupes a victim into opening an email, instant message, or text message (Goel & Jain, 2018; Gupta et al. 2017; Jakobsson & Myers 2006; Pienta et al., 2018; Thakur et al., 2015; Wright et al. 2014). The recipient is then tricked into clicking a malicious link, thereby triggering undesirable processes such as malware installation or a system freeze as part of a

ransomware attack; most commonly, the victim is induced to reveal sensitive personal or account information (Thakur et al., 2015). Phishing attacks can be quite sophisticated, making it difficult for spam filters and other cybersecurity tools to defend against them (Pienta et al., 2018), and they can result in substantial financial loss for individuals or organizations (Goel & Jain, 2018).

Given the prevalence of these attacks, coupled with the fact that they require the victim to collaborate with the offender, cybersecurity experts are increasingly seeking to raise public awareness of the nature of phishing attacks and the risks involved (Gallo et al. 2024; Goel & Jain, 2018; Gupta et al. 2017; Li et al. 2019; Pienta et al., 2018; Wong et al. 2022). Information systems (IS) researchers have likewise devoted considerable efforts to characterizing phishing attacks and identifying ways to prevent them. For example, studies have investigated the effects of overconfidence on phishing detection (Wang et al. 2016), attention-reallocating techniques to prevent phishing (Jensen et al. 2017), the role of gender and other individual characteristics in phishing avoidance behavior (Verkijika, 2019), and cybersecurity compliance behavior in organizations (Li et al. 2019). Particularly relevant to these

* Corresponding author.

E-mail addresses: nami@cmu.edu (N. Ilany-Tzur), finkl@bgu.ac.il (L. Fink).

<https://doi.org/10.1016/j.ijinfomgt.2025.102919>

Received 1 July 2024; Received in revised form 29 April 2025; Accepted 4 May 2025

Available online 19 May 2025

0268-4012/© 2025 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

efforts is an IS theory called technology threat avoidance theory (TTAT), which aims to understand users' risk-avoidance behavior in technological contexts (e.g., [Liang & Xue, 2009](#)). This theory posits that individuals' perceptions influence their awareness and, consequently, their motivation to avoid risk ([Carpenter et al. 2019](#)).

Herein, we contribute to this stream of IS research by examining a potential determinant of users' online risk-avoidance behavior that has received little attention to date: The device on which the user is browsing, i.e., a mobile device, and specifically a smartphone ("mobile"), versus a personal computer (PC). In general, research has demonstrated that the decision-making behavior of mobile users is different from that of PC users. For example, studies have shown that, compared with PC users, mobile users (i) perform more poorly on cognitive tasks that demand high cognitive load ([Ilany-Tzur & Fink, 2022](#)); (ii) rely more extensively on recommendation systems in retail ([Lee et al., 2020](#)); and (iii) exhibit less exploratory behavior when browsing commercial websites ([Raphaelli et al. 2017](#)). Furthermore, research has also demonstrated that decision-making behavior or styles have an influence on risk-avoidance behavior ([Donalds & Osei-Bryson, 2020](#)). While researchers have investigated phishing attacks in a mobile context (e.g., [Goel & Jain, 2018](#)), there remains a gap in the literature regarding the unique implications of the mobile context for risk-avoidance behavior, and how device usage (i.e., mobile vs. PC) relates to vulnerability to cybersecurity attacks in general, and to phishing attacks in particular.

To narrow this gap, between existing knowledge on how mobile usage impacts decision making and understanding of how contextual factors influence risk-avoidance behavior, we addressed the following research question: How do mobile users differ from PC users in terms of their risk-avoidance behavior in the context of cybersecurity and, specifically, phishing? By addressing this research question, we advance the understanding of how an important contextual factor in contemporary use-environments, specifically the device being used, affects risk-avoidance behavior, specifically susceptibility to phishing attacks.

In terms of the research design, our research comprises three studies. Study 1 is based on an analysis of field data from a cybersecurity company that provides security solutions for internet service providers (ISPs). We analyzed anonymized data about online user behavior in a sample of households, including data about the device being used and the level of risk associated with each click performed with these devices. Our results suggest that risk-avoidance behavior differs significantly between PC users and mobile users—specifically that mobile use is associated with more risk-avoidant behavior compared with PC use.

As the findings of this analysis are limited by the endogeneity of device choice, and to address the limitations of the nonexperimental methods of Study 1 in providing a causal explanation of the behavioral effects of the device ([Fink, 2022](#)), we subsequently conducted two controlled online experiments (Studies 2 and 3), wherein users' device and risk levels were assigned exogenously for a certain task, in which users were exposed to a simulated phishing attack. Results support the findings of Study 1, indicating that mobile users show a stronger tendency than PC users to avoid clicking on a potentially risky link. Notably, this difference was observed primarily for lower-risk links (where risk level was determined by a pre-test). In the presence of higher-risk links, mobile users and PC users showed similar levels of risk-avoidance behavior. Overall, these findings inform our understanding of how risk-avoidance behavior of users varies across devices, thereby highlighting important boundary conditions for the susceptibility of users to cybersecurity risks.

2. Theoretical background and research hypotheses

2.1. Phishing attacks and privacy behavior

Information security research and practice have provided a general understanding of phishing attacks and ways to defend against them

([Birthriya et al., 2025](#); [Pienta et al., 2018](#)). Research efforts in this regard, among other aspects, have focused on detection strategies ([Zahedi et al. 2024](#)) and identifying phishing attacks with high accuracy ([Berens et al. 2024](#)), characterizing attack techniques, and identifying appropriate defense mechanisms ([Goenka et al. 2024](#); [Gupta et al. 2017](#)). Most phishing defense techniques rely on enhancing users' awareness of such attacks and their ability to avoid clicking malicious links by offering various sets of rules to follow ([Davis et al. 2025](#); [Goel & Jain, 2018](#); [Gupta et al. 2017](#); [Pienta et al., 2018](#); [Wong et al. 2022](#)). Cybersecurity research has also focused on improving individuals' security compliance behavior, showing that users' decision-making style significantly influences their cybersecurity behavior ([Donalds & Osei-Bryson, 2020](#)). Recent research suggests that employees exhibiting excessive optimism are more likely to engage in insecure behaviors ([Owen et al., 2024](#)). However, research is still in its early stages concerning how people actually behave when exposed to a phishing attack, and which defense mechanisms they might deploy. An understanding of these behavioral elements is important because, in many cases, a phishing attack is successful only if users (unbeknownst to them) collaborate with the attack and provide some personal information (i.e., if information disclosure takes place).

Notably, extensive IS research has focused on users' information disclosure behavior, albeit outside the specific domain of phishing. Much of this research adopts the framework of the privacy calculus model ([Smith et al. 2011](#)), which conceptualizes information disclosure behavior as an outcome of a cost-benefit analysis. This model assumes that users faced with an information disclosure decision compare perceived risks—also mediated by perceived trust and perceived privacy concerns—against perceived utilities, and, on the basis of this comparison, they decide to disclose or withhold private information ([Dinev & Hart, 2006](#)). When the perceived risks are lower than the perceived utilities (which may occur in the presence of low privacy concerns or high trust in the entity requesting the information), the resulting behavior will be disclosure. When perceived risks are higher than perceived utilities, users will withhold information.

Research in this vein has also described a phenomenon referred to as the privacy paradox, in which users' stated risk preferences are inconsistent with their information disclosure behavior ([Acquisti & Grossklags 2012](#); [Pavlou, 2011](#)). Three main factors have been suggested to explain the privacy paradox ([Acquisti et al. 2015](#)): (i) users' uncertainty regarding the consequences of their privacy-related behaviors and regarding their preferences over these consequences, (ii) context dependency of users' privacy perceptions and behaviors, and (iii) malleability of the privacy calculus—such that users' considerations can be influenced by commercial, governmental, or even criminal interests. For the purpose of this study, the notion that privacy-related behavior is characterized by uncertainty and malleability seems particularly relevant because deception is an integral part of phishing attacks.

Applying these ideas to a phishing scenario, we can say that phishing entails fraudulent manipulation of a user's privacy calculus. That is, the attacker elicits a false expectation of utility (e.g., a promise of a monetary benefit that will never materialize), while simultaneously interfering with the user's perceptions of the risk—by actively taking steps to hide malicious intentions and to enhance the user's trust (e.g., by sending a message from an address that appears to belong to a trusted institution). Differences in individuals' tendencies to fall victim to such attacks may thus be explained by various individual characteristics such as detection ability, response bias (i.e., basic tendency to assume that any given message is a malicious attack), confidence, and perception of consequences ([Canfield et al. 2016](#)). In particular, the current study proposes that the decision to comply with a fraudulent request relies on users' likelihood of perceiving a phishing message as risky. Crucially, we suggest that an individual's tendency to perceive and avoid risk is influenced, among other aspects, by the device he or she is using. In what follows, we further discuss the notion of risk avoidance, particularly in technological contexts, and the potential role of devices in

risk-avoidance behavior.

2.2. Risk-avoidance behavior

Risk is a multidimensional construct (Ou et al. 2022). It is generally well established that people differ in the extent to which they engage in risky behaviors. A key factor driving these differences is inherent risk aversion—a term that originated in the field of economics and refers to people's tendency to prefer outcomes with low uncertainty to those with high uncertainty, even if the expected value of the latter is equal to or higher than the expected value of the more certain outcome (Kahneman & Tversky, 1979). The roots of the academic discussion on risk aversion date back to 1738 when Daniele Bernoulli published an article attempting to explain why people avoid risk and proposing that risk aversion diminishes with wealth (Kahneman & Tversky, 2000). Since then, risk aversion has gained a central place in economic theory. Indeed, economists have a simple and elegant explanation for it, which is derived from the expected utility maximization of a concave utility-of-wealth function (Rabin & Thaler, 2001).

Whereas risk aversion is a personal tendency or trait, and thus presumably stable across different contexts, risk avoidance—which manifests in the actual choices that people make—is a behavioral outcome that can vary as a result of contextual changes. For example, previous findings have indicated that the extensiveness of information in one's environment is positively associated with trust (Furner & Zinko, 2017), and that trust is negatively associated with perceived risk (Hansen et al., 2018; Yang et al. 2015). Thus, people's perception of the risk associated with a given action, and thus their likelihood of avoiding that action, may depend on the amount of information at their disposal pertaining to that action.

In IS, the above-mentioned theory called TTAT has emerged to explain users' divergent responses to risks in technological contexts. This theory posits that users are motivated to avoid malicious information technology (IT) when they (i) perceive a threat and (ii) believe that they can avoid that threat by taking safeguarding measures (Liang & Xue, 2009). According to TTAT, avoidance behavior depends on risk appraisal, a process in which users assess the risk of malicious IT based on their perceived susceptibility to it and the perceived severity of the malicious IT. Risk appraisal is affected by risk tolerance (a main independent factor that affects risk appraisal and can be understood as essentially the complement of risk aversion), which, in technological contexts, can be understood as the minimum discrepancy between the undesired end state (to be attacked by malicious IT) and the current state that users can tolerate (Liang & Xue, 2009). Users' risk tolerance has a negative effect on their threat perceptions, such that, when facing the same malicious IT, a more risk-tolerant user will perceive a lower degree of a threat than a less risk-tolerant one (Liang & Xue, 2009). Notably, though studies adopting the lens of TTAT have addressed personal characteristics—such as risk tolerance—that affect overall threat perceptions and subsequent risk-avoidance behavior (Carpenter et al. 2019), there is a gap in the TTAT literature regarding the role of contextual variables in these outcomes. The current study addresses this gap by focusing on device usage as a contextual factor that might influence users' risk-avoidance behavior. Clearly, the device is a critical contextual factor in understanding the tendency of users to avoid technology threats, particularly if they vary in their responses to similar threats on different devices.

2.3. Device usage and user behavior

In the past two decades, there has been a momentous shift from the PC to the smartphone as the device of choice for various online activities (Ghose, 2017; Levi-Bliech et al. 2019; Piccoli & Ott, 2014; Pousttchi et al. 2015). Researchers have devoted considerable attention to mobile devices, investigating the determinants of mobile use (Gerpott & Thomas, 2014; Liu et al. 2019), mobile users' commerce behavior

(Pavlou et al., 2007), and mobile users' privacy concerns (Degirmenci, 2020). Several studies have compared different devices to investigate how the physical characteristics of a device (e.g., screen size and interface design) affect various user-related outcomes, including navigation behavior (Chae & Kim, 2004); satisfaction, trust, and loyalty to the device manufacturer (Lee et al. 2015); effectiveness of video-based learning (Maniar et al. 2008); effectiveness of information search (Sweeney & Crestani, 2006); and effectiveness of recommendation agents (Ravula et al., 2024).

Several works have directly compared the behavior of mobile users with that of users of non-mobile devices, particularly in consumption-related domains (e.g., e-commerce browsing and purchasing behavior: Raphaelli et al. 2017; Xu et al. 2016; electronic word of mouth: Burtch & Hong, 2014; Piccoli & Ott, 2014). Studies in this stream suggest, for example, that mobile users exhibit less exploratory behavior than PC users when browsing commercial websites (Raphaelli et al. 2017). Other studies have shown that mobile users make less accurate consumer choices (Fink & Papismedov, 2023). Recent findings suggest that such discrepancies may be attributable to the fact that mobile users are prone to more heuristic information processing, leading to lower decision accuracy, particularly under conditions of high cognitive load (Ilany-Tzur & Fink, 2022).

Notably, findings of a study by Ghose et al. (2013) suggest that, compared with PC users, mobile users may be more responsive to digital cues. Specifically, the authors found that mobile users (i) are more responsive to ranking effects (i.e., they have a stronger tendency to click on messages or search results that are closer to the top of a list), suggesting that mobiles have higher search costs; and (ii) have a stronger tendency to click on messages from geographically close entities, suggesting that “distance matters more” to mobile users. The authors suggested that, because of these features, “the mobile Internet is somewhat less ‘Internet-like’” (Ghose et al. 2013, p. 499). This suggestion can imply that the “mobile internet” can be interpreted as a different context. Applying these findings to our context, we suggest that mobile users might have a more powerful response than PC users to digital cues indicative of risk—an idea we expand on below.

2.4. Hypotheses

Here, building on the theory (put forward in TTAT) that users' risk perceptions are malleable (Liang & Xue, 2009), we propose that device usage is likely to influence users' risk-avoidance behavior in response to risk cues. In particular, we suggest that, when faced with similar risk cues, PC users are likely to engage in riskier behavior compared with mobile users. These differences in behavior are the consequence of differences in users' ability to engage in accurate risk assessment across devices. Specifically, mobile users should find it more demanding to accurately assess the risk associated with a specific cue relative to the assessment of the same cue by PC users. This view is consistent with the notion of higher search costs in mobile use (Ghose et al. 2013). This notion that information search costs for mobile users are higher than information search costs for PC users suggests that there are higher payments or demands for mobile users in comparison to PC users and that it is costlier to accurately assess the level of risk associated with a cue when the screen with which the user interacts is smaller and less information is presented on a single page (Fink & Papismedov, 2023). This view is also consistent with the notion that the environment typical of mobile use is more constrained in terms of the ability of users to devote substantial cognitive resources to the task at hand (Ilany-Tzur & Fink, 2022). Both the smaller device and the more constrained environment serve as contextual mechanisms that increase the difficulty of risk assessment for mobile users. Because these users are more likely to feel that assessing risk is a costly and demanding task and that they are in an environment wherein they are unable to adequately assess the risk associated with a specific cue, they are more likely to revert to the default behavior of avoiding the risk, typical of their behavior in cases of

high risk. In contrast, PC users are more likely to feel that they can adequately evaluate the risk, given that they are interacting with a larger screen and are in an environment that is less cognitively constraining, culminating in a greater likelihood of accepting the risk. Consequently, we expect mobile users to be less inclined to take risks in their browsing behavior and more inclined to opt for avoidance as a way of mitigating potential risks. This depiction is consistent with findings of greater perceived risk in mobile use relative to PC use according to subjective data collected in the Canadian Internet use survey (Cozzarin & Dimitrov, 2016). It is also consistent with findings that mobile users display less exploratory behavior than PC users in browsing commercial websites (Raphaelli et al. 2017). Moreover, it is also consistent with research on the antecedents of risk-avoidance behavior (Donalds & Osei-Bryson, 2020). Based on this reasoning, we hypothesize that mobile users are more likely than PC users to display risk-avoidance behavior.

Hypothesis 1. (H1): *Mobile users are more likely than PC users to display risk-avoidance behavior.*

An important implication of H1 is that mobile users are more likely than PC users to display avoidance behavior typical of the way users respond to risky cues, irrespective of the actual risk of the specific cue they encounter. Because mobile users find it more demanding to assess the risk of a cue, they are more likely to display risk-avoidance behavior not only in the case of higher-risk cues, but also in the case of lower-risk cues. In other words, because mobile users perceive higher search costs in estimating the risk associated with a cue, implying that they are more likely to revert to the default behavior of avoiding the risk, these users are also expected to be less sensitive to the risk level of a cue, and their risk-avoidance behavior is likely to reflect this lower sensitivity. By comparison, PC users, who find it less demanding to engage in risk assessment, can be more sensitive to the risk level of a cue, thereby displaying greater risk-avoidance behavior with higher-risk cues than with lower-risk cues. PC users perceive lower search costs in estimating the risk associated with a cue and, therefore, are better positioned to estimate the risk and adequately respond to it. This reasoning suggests that risk-avoidance behavior is affected by the interaction between device usage and risk level. According to this interaction effect, the risk level is expected to have a positive effect on risk-avoidance behavior (i. e., greater avoidance when the risk is higher) only in PC use. In mobile use, by contrast, risk-avoidance behavior is expected to be relatively high, with little effect of risk level on risk-avoidance behavior. Consequently, we expect the effect described in H1, according to which mobile users are more likely than PC users to display risk-avoidance behavior, to be more evident for lower-risk cues, for which PC users are expected to be less risk avoidant. Conversely, for higher-risk cues, mobile users and PC users are expected to display more similar risk-avoidance behavior, consistent with the actual level of risk of the cue. This differential response to higher-risk versus lower-risk cues as a function of device usage is described in our second hypothesis.

Hypothesis 2. (H2): *The differences in risk-avoidance behavior between mobile users and PC users are greater for lower-risk cues than for higher-risk cues.*

To empirically test these hypotheses, we conducted three studies. Study 1 was a field data analysis aimed at testing H1 to confirm the fundamental effect of device usage on risk-avoidance behavior with real-world clickstream data prior to engaging in the design of controlled online experiments and the resource-consuming development of online platforms for these experiments. Study 2 was a controlled online experiment aimed at testing both hypotheses in a setup in which the device was exogenously manipulated rather than self-selected by users, thereby providing the methodological foundation necessary to infer about the causal effects of device usage, either as a main effect (H1) or as an interaction with risk level (H2), on risk-avoidance behavior. Study 3 was a conceptual replication of Study 2 and aimed at establishing the robustness of the effects observed in Study 2 with a different

experimental task.

3. Study 1: field data analysis

3.1. Methodology and data collection

To test H1, we collaborated with a cybersecurity start-up company that develops security solutions for small (“home” or “domestic”) networks. The company provides business-to-business (B2B) services to Internet service providers and communication companies. As part of its service, and with the purpose of detecting internet crimes, the company monitors all URL requests originating from all devices connected to each of the domestic networks it serves.

The company provided us with access to anonymized records of URL requests according to the following procedure. First, we randomly selected 30 domestic networks from an anonymized list of networks monitored by the company. Then the company provided us with all available records of the URL requests that originated from these networks during one week in 2020, from August 30 to September 5. (We note that this data set is a random partial sample of the complete set of requests that the company received from the focal networks, as the company randomly deletes some of its data due to storage issues. Furthermore, we note that we obtained Wi-Fi traffic generated by network devices; not cellular traffic). Because the company monitors all URL requests originating from all devices connected to each specific domestic network, we excluded all requests originating from devices that were not PCs or mobiles, including Internet-of-Things (IoT) devices, tablets (our data indicated a low volume of tablet use), smart televisions, and so on. Next, we randomly sampled about half a million URL requests from the remaining requests. Ultimately, the data set analyzed in this study included 499,781 observations, constituting a random sample of the stream of URL requests made by PC and mobile devices connected to the 30 focal networks during a period of one week.

For each URL request, we obtained data about the following five variables:

- I. Safety level of the target URL—a binary variable with “0” indicating an unsafe URL address and “1” indicating a safe URL address. Classification of a URL as unsafe or safe was based on safety scores calculated by BrightCloud Threat Intelligence, a company that provides safety ratings for URLs based on forecasts of their security risks, producing a safety score on a scale from 0 to 100. Because the distribution of these scores for our URLs was multimodal, we transformed this scale into a binary indicator, with the cutoff determined based on industry common practices (values below 40 were considered unsafe).
- II. Device—a binary variable with “0” indicating a URL request that originated from a PC and “1” indicating a URL request originating from a mobile.
- III. Network size—an integer that represents the number of devices connected to the network from which the URL request originated.
- IV. Mobile percentage—a number between 0 and 100 representing the percentage of mobiles out of the total number of devices connected to the network from which the URL request originated.
- V. Use frequency—a binary variable with “0” indicating a URL request that originated from a device that was infrequently used (two days or less during the week) and “1” indicating a URL request originating from a device that was frequently used (more than two days during the week).

Descriptive statistics for these variables are presented in Table 1.

This dataset of URL requests captures the real-time stream of browsing activity, reflecting dynamic user behavior as manifested through actual interactions with URLs on domestic networks.

Table 1
Descriptive statistics for Study 1.

Variable	Mean	Median	Mode	St. dev.	Quartile 1	Quartile 3
Safety level of target URL (unsafe = 0, safe = 1)	0.974	1	1	0.159	1	1
Device (PC = 0, mobile = 1)	0.785	1	1	0.411	1	1
Network size (Number of devices on network)	8.245	8	10	4.082	6	10
Mobile percentage (Percentage of mobiles per network devices)	64.570	62.5	50	17.551	50	75
Use frequency (low = 0, high = 1)	0.979	1	1	0.143	1	1

3.2. Results

To test H1, we estimated a mixed-effects logistic regression model, with the safety level of the target URL as the explained variable. The unit of analysis was the URL request. The model included fixed effects for the device, network size, mobile percentage, and use frequency, as well as for all two-way interactions of the device with other variables. The model also included a random effect for the network. The results of the model estimation are presented in Table 2.

The model estimation results show a positive and significant relationship between mobile device and the safety level of the target URL ($p < .001$); this effect is also the largest in size of all tested effects. Specifically, the effect size implies that the odds ratio of clicking a safe (rather than unsafe) URL address for a mobile is 4.02 times that for a PC. This result supports our hypothesis that mobile users display a higher level of risk avoidance compared with PC users (H1). It is also noteworthy that the size of the network is significantly negatively associated with the safety level of the URL address requested ($p < .001$), implying that devices on larger networks are more prone to accessing unsafe URLs. Finally, it is also evident that all two-way interactions are significant ($p < .05$ in all cases), showing that the positive relationship between mobile device and target URL safety is stronger for networks with more devices, for networks with a smaller share of mobile devices, and for devices that are frequently used.

Table 2
Mixed-effects logistic regression model results for Study 1.

	Target URL safety (unsafe = 0, safe = 1)
Intercept	3.687 *** (0.152)
Device (mobile)	1.393 *** (0.132)
Network size	-0.156 *** (0.027)
Mobile percentage	0.002 (0.004)
Use frequency (low)	0.014 (0.052)
Device (mobile) × network size	0.197 *** (0.007)
Device (mobile) × mobile percentage	-0.007 * (0.002)
Device (mobile) × use frequency (low)	-0.449 *** (0.108)

$N = 499,781$; Unstandardized coefficients are shown, with standard errors in parentheses; $^+ p < 0.1$; $* p < 0.05$; $** p < 0.01$; $*** p < 0.001$.

4. Study 2: a controlled experiment

Study 1 provided initial support for our proposition that mobile users tend to be more risk-avoidant than PC users, as reflected in their greater tendency to access safe (vs. unsafe) URLs. Yet, a notable shortcoming of Study 1 is the endogeneity of device choice, as users in our field setting were able to self-select the devices with which they made URL requests. A complementary approach for non-experimental methods is the use of online controlled experiments, which provide the methodological infrastructure necessary to infer about causal effects (Fink, 2022). In Study 2, we sought to address this concern about self-selection in Study 1 by performing a randomized online experiment to test the causal effect of the device on risk-avoidance behavior in a controlled environment. In this experiment, we also tested whether users responded differentially to high-risk versus low-risk links as a function of device use (H2).

4.1. Methodology

4.1.1. Participants and design

For Study 2, we designed and developed a designated platform that facilitates controlled online experiments. Participants entered the platform remotely, from their own environment using their own devices, and were asked to perform a digital task while their performance and the entirety of their behavior as manifested in their clickstream and the corresponding timestamp for each click was measured and monitored. We recruited workers ($n = 257$; 43 % female) from the Amazon Mechanical Turk (AMT) platform. After entering the website using a unique code they received from AMT and signing a consent form, the participants were asked to perform an image tagging task. Given the high popularity of such tasks in AMT, this task simulated a natural environment for these AMT workers. Each participant was assigned a particular version of an image tagging task. During the task, we simulated a phishing attack: Participants received a popup message asking them to click on a certain link. The dependent variable was whether a participant avoided clicking on the link (indicating risk-avoidance behavior).

The version of the task that each participant viewed corresponded to one of eight experimental conditions, to which they were randomly assigned in a $2 \times 2 \times 2$ between-subjects design comprising the device type used by the participant (mobile vs. PC), the risk level of the link in the popup message (high-risk vs. low-risk), and the complexity level of the task (high-complexity vs. low-complexity). Task complexity was included as an additional independent variable to explore whether the effects described in H1 and H2 were sensitive to the cognitive demands of the task, particularly because our hypotheses are based on the reasoning that mobile use represents a more cognitively constrained environment. User behavior was recorded by the website, enabling us to compare risk avoidance between mobile and PC users, contingent on the risk level.

4.1.2. Procedure

Each participant was sent a message on the AMT platform that indicated which device he or she should use to access the task. Device assignment was random, thereby ensuring that this variable was exogenous. The participant then accessed the designated website from a device of that type. The website automatically verified that participants were using the devices corresponding to their assigned conditions using the unique code they received from AMT. For example, if a participant was assigned to one of the four mobile groups, the system identified this assignment via the code and then verified that each of their HTML requests originated from a mobile device.

After accessing the website, each participant was presented with a picture-tagging task with a level of complexity corresponding to his or her complexity condition. In this task, the participant viewed 12 pictures, one after the other, and was asked to identify or count the items in each picture. For each picture, the participant had to choose the correct answer in a multiple-choice manner. Table 3 shows examples of pictures

Table 3
Examples of tasks with different complexity levels for Study 2.

Task complexity level:	Low	High
The picture presented:		
The question:	What is in the picture?	How much money is in the picture?

and questions used in the simple and complex versions of the task.

After participants were shown the twelfth picture (and without being informed that they had reached the end of the task), they were shown a popup message containing text and a link, i.e., a URL. All popup messages had the same text, but the featured URLs conveyed different levels of risk (i.e., high or low), in accordance with participants' assigned risk conditions.

To select the URLs corresponding to the different risk conditions, we relied on a pre-test. Specifically, in this pre-test, we used another designated website that featured a rating task of 20 popup messages resembling the ones used in our main study with identical text and different URLs. Participants ($n = 30$) were recruited via the AMT platform and were asked to rate the risk level of each message on a scale of 1–100. We then used a t -test to compare the average ratings of the top four and the bottom four URLs, and found that the differences between the two groups were statistically significant. Thus, we categorized the four URLs that had received the lowest risk rate as “low-risk” and the four URLs that had received the highest risk rate as “high-risk”. To avoid any effects that might be caused by a specific URL, we used the entire pool of eight messages, and randomly presented each participant with a specific message among the four in the risk category s they were assigned to.

The popup message—shown in Fig. 1—was deliberately framed to be unrelated to the task. The code was designed to make sure that the popup message destination (browser tab) would be identical for all

participants. Participants who clicked the link were transferred to a webpage containing the following message: “Oops... This link is broken. Please go back to the source.”

In a final step, participants filled out a demographic questionnaire containing items such as gender, age, education, and device literacy.

4.2. Results

To test H1 and H2, we estimated a logistic regression model, with risk avoidance—i.e., avoiding clicking the link—as the explained variable (0 = participant did not avoid clicking, 1 = participant avoided clicking). The unit of analysis was the user. The model included fixed effects for device (1 = mobile; 0 = PC), URL risk level (1 = high; 0 = low), and task complexity level (1 = high; 0 = low), as well as for the two-way interaction of the device with the URL risk level. The model also included fixed effects for mobile literacy and for PC literacy as control variables. The results of the model estimation are shown in Table 4.

The results show that the effect of device on avoidance behavior was positive and significant ($p < .05$), with a coefficient of 0.985, implying that mobile users were 2.67 times more likely than PC users to show risk-avoidant behavior, i.e., to avoid clicking the link presented in the popup. This finding lends support to H1 and is consistent with the findings of Study 1 regarding mobile users' heightened tendency (as compared with PC users) to access safe (vs. unsafe) URLs.

While URL risk level did not affect avoidance behavior on its own, the interaction effect between device and URL risk level was significant

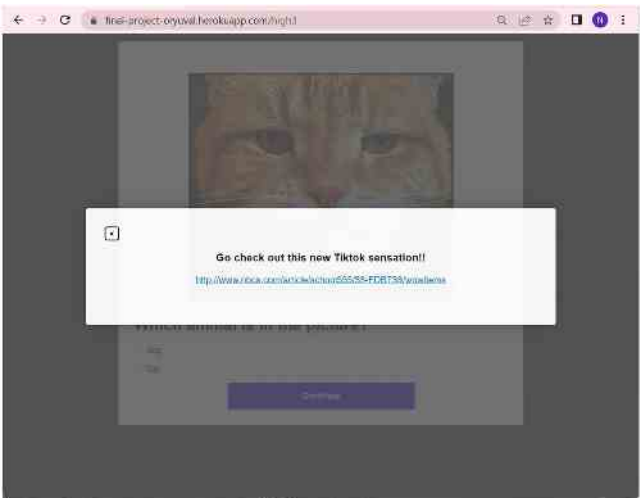


Fig. 1. Popup message example.

Table 4
Logistic regression model results for Study 2.

	Model term
(Intercept)	0.545 (0.527)
Device (1 = mobile; 0 = PC)	0.985 * (0.407)
URL risk level (1 = high; 0 = low)	0.334 (0.373)
Device × URL risk level	−0.915+ (0.550)
Task complexity level (1 = high; 0 = low)	0.041 (0.280)
PC literacy	0.177 (0.162)
Mobile literacy	−0.304+ (0.171)

$N = 257$; Unstandardized coefficients are shown, with standard errors in parentheses; + $p < 0.1$; * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$.

at the 0.1 level. According to Fig. 2, which depicts this interaction effect, in the high-risk condition, mobile users did not substantially differ from PC users in terms of their risk-avoidance behavior. However, in the low-risk condition, mobile users showed a stronger tendency towards risk-avoidance behavior than did PC users. Indeed, the results of pairwise comparisons, reported in Table 5, show that the difference between mobile users and PC users was not significant in the high-risk condition ($p = 0.852$), whereas it was significant in the low-risk condition ($p = 0.015$). (Similar pairwise comparisons between low-risk and high-risk conditions for each device showed that these differences were nonsignificant.) These findings lend support to H2 about the differences in risk-avoidance behavior between mobile users and PC users being greater for lower-risk cues than for higher-risk cues.

Finally, the effects of task complexity level and PC literacy on risk-avoidance behavior were not significant. The effect of mobile literacy on risk-avoidance behavior was negative and significant at the 0.1 level, implying that participants who reported using mobile devices to a greater extent were more likely to click on the link in the popup compared with participants who used mobile devices less extensively.

5. Study 3: a second controlled experiment

To lend further support to the results of Studies 1 and 2, we conducted an additional controlled online experiment, similar to the one in Study 2—but with a different picture tagging task, as elaborated below.

5.1. Methodology

For this experiment, we recruited 256 participants (30 % female) from AMT. The experimental design and procedure were identical to those described for Study 2, except that, in this study, we used an image recognition task inspired by Shane Frederick's (2005) cognitive reflection test, in which image complexity was manipulated in a different manner. Specifically, in this task, participants were asked to identify whether each picture contained a dog or a cat. Participants in the low-complexity condition viewed a clear version of the picture, whereas participants in the high-complexity condition viewed a blurred version of the picture (see example in Table 6).

5.2. Results

We estimated the same logistic regression model described in Study 2, with the same dependent variable (avoidance behavior, i.e., avoiding clicking a link) and explanatory variables (device, URL risk level, interaction of device with URL risk level, task complexity level, and device literacy variables). Again, the unit of analysis was the user. The results of model estimation are presented in Table 7.

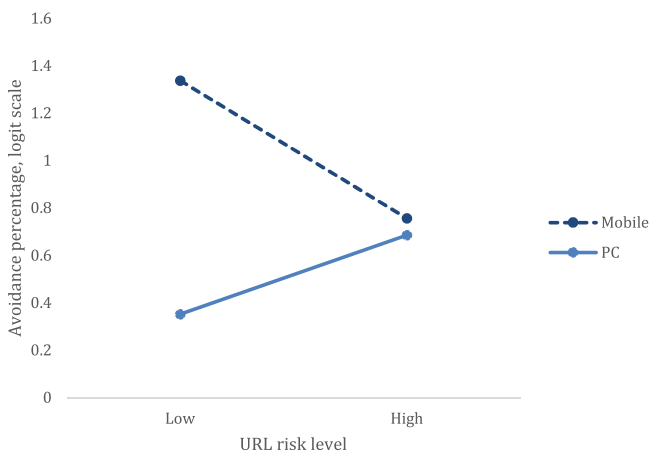


Fig. 2. Effect of URL risk level and device on risk-avoidance behavior; Study 2.

Table 5

Pairwise comparisons for Study 2.

Contrast	Risk level	Estimate	Standard Error	Z-ratio	p-value
PC - Mobile	Low	-0.989	0.407	-2.427	0.015
PC - Mobile	High	-0.072	0.385	-0.187	0.852

Results are averaged over task complexity level. Estimates are given on the logit (not the response) scale.

The results of model estimation once again reveal a positive and significant effect of device on risk-avoidance behavior ($p < .001$). The coefficient of 1.490 implies that mobile users were 4.43 times more likely than PC users to avoid clicking the popup link. This finding is consistent with the results of Study 1 and Study 2, and lends further support to H1.

We further observe that, as in Study 2, URL risk level did not significantly affect risk-avoidance behavior. In this study, however, unlike in Study 2, the regression coefficient for the interaction of the URL risk level with the device was not statistically significant (similar to the coefficients for the task complexity level and both device literacy variables). The interaction effect of the URL risk level with the device on risk-avoidance behavior is depicted in Fig. 3. Though this interaction effect was not statistically significant in our model estimation, the figure reveals patterns similar to those observed in Study 2. Specifically, the differences in risk avoidance between devices are smaller in the high-risk condition than in the low-risk condition. Notably, the results of pairwise comparisons, presented in Table 8, are consistent with those in Study 2: The difference between mobile users and PC users was not significant in the high-risk condition ($p = 0.195$), whereas it was significant in the low-risk condition ($p = 0.006$). These results of Study 3 provide evidence in support of H2.

6. Discussion

6.1. Key findings

This research aimed to empirically investigate the effect of device usage (mobile vs. PC) on users' risk-avoidance behavior and, specifically, on the tendency to avoid potentially risky links similar to those deployed in phishing attacks. In Study 1, we analyzed field data, corresponding to half a million URL requests in a sample of home networks, to identify associations between device usage and users' risk-avoidance behavior, operationalized as the users' tendency to access safe (vs. unsafe) URLs. This analysis showed that, in line with H1, mobile users displayed a higher level of risk-avoidance behavior compared with PC users. This counterintuitive finding seems to challenge the prevailing belief that the increased cost of risk assessment associated with mobile device usage would cause users to act more recklessly and take on greater risks. In contrast, our results reveal the opposite effect: The higher cost of risk assessment on mobile devices prompts users to adopt a more risk-averse behavior, seemingly relying on a "better to be safe than sorry" heuristic and embracing a more cautious, risk-avoidant approach.

To establish the causal nature of this association, as well as to explore users' sensitivity to risk cues of different severity levels (H2), we conducted controlled online experiments in which device usage and risk cues were randomly assigned. Both Studies 2 and 3 showed that, in line with H1 and the results of Study 1, mobile users showed stronger risk avoidance than PC users did (as reflected in users' tendency to avoid clicking on a link featured in a popup resembling a phishing message). Notably, in these two studies, we can infer causality and conclude that device usage is responsible for the differences in risk-avoidance behavior. Furthermore, we can conclude that, in line with H2, sensitivity to differential risk levels is dependent on device usage. Specifically, Study 2 showed a significant interaction effect of risk level and device on risk-avoidance behavior (though this effect was not

Table 6

Examples of tasks with different complexity levels for Study 3.



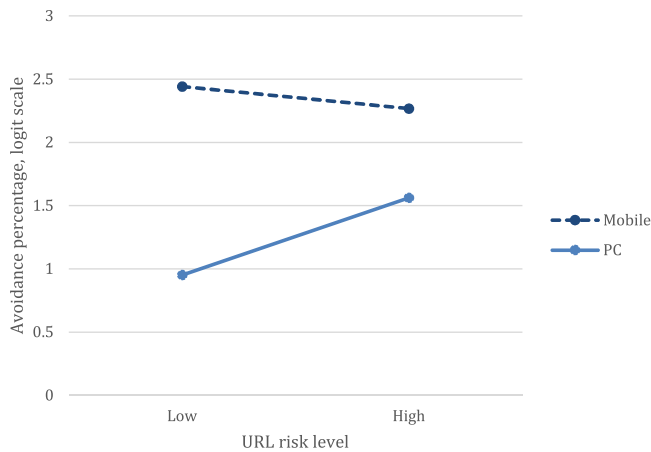
Task complexity level:	Low	High
The picture presented:		
The question:	Is it a cat or a dog?	Is it a cat or a dog?

Table 7

Logistic regression model results for Study 3.

	Model term
(Intercept)	0.312 (0.770)
Device (1 = mobile; 0 = PC)	1.490 * ** (0.546)
URL risk level (1 = high; 0 = low)	0.611 (0.433)
Device × URL risk level	−0.785 (0.768)
Task complexity level (1 = high; 0 = low)	0.066 (0.353)
Mobile literacy	−0.091 (0.233)
PC literacy	0.295 (0.213)

$N = 256$; Unstandardized coefficients are shown, with standard errors in parentheses; $^+ p < 0.1$; $^* p < 0.05$; $^{**} p < 0.01$; $^{***} p < 0.001$.

**Fig. 3.** Effect of URL risk level and device on risk-avoidance behavior; Study 3.**Table 8**

Pairwise comparisons for Study 3.

Contrast	Risk level	Estimate	Standard Error	Z-ratio	p-value
PC - Mobile	Low	−1.490	0.546	−2.730	0.006
PC - Mobile	High	−0.705	0.545	−1.295	0.195

Results are averaged over task complexity level. Estimates are given on the logit (not the response) scale.

statistically significant in Study 3). Moreover, in both Studies 2 and 3, pairwise comparisons showed that mobile users exhibited a higher rate of risk avoidance than PC users only when the risk level was low. When the risk level was high, both mobile and PC users were similarly reluctant to take the risk of clicking on a popup message. This interaction effect provides further support for our conclusion that mobile users address the higher cost of risk assessment by avoiding the risk rather than by succumbing to it.

The findings of all three studies provide empirical evidence in support of the contextual nature of risk-avoidance behavior, suggesting that mobile use settings may constrain the ability of users to engage in risk assessment, possibly causing their behavior to be more avoidant than necessary when links pose no significant risk. In contrast, PC use settings may be more suitable for engaging in risk assessment, allowing users to respond in a manner that is more consistent with the actual level of risk. This pattern of greater risk-avoidance behavior in mobile use, particularly for lower-risk links, is observed in real-world clickstream data when users self-select their devices (Study 1) and in the behavior of participants in two different image tagging tasks when the device is exogenously determined for users (Studies 2 and 3). The robustness of these findings across the different studies and setups strengthens both the internal and external validity of our findings.

6.2. Theoretical contributions

This work makes important contributions to IS research on mobile use and on risk-avoidance behavior. First, we advance the literature on mobile use by revealing important behavioral differences between mobile users and PC users. We propose, and empirically confirm, that mobile users are more likely than PC users to avoid risk in their web-browsing behavior. Notably, mobile users' tendency towards risk avoidance may constitute a plausible explanation for prior observations that mobile users exhibit less exploratory behavior than PC users when interacting with commercial websites (e.g., [Raphaelli et al. 2017](#)).

Second, we contribute to IS research on risk avoidance, and specifically to TTAT, by identifying device usage as a contextual factor that can influence risk-avoidance behavior. As discussed in previous sections, TTAT posits that avoidance behavior is determined by a risk appraisal process in which users assess the severity of the risk and their susceptibility to it. Though TTAT research has explored personal characteristics that might influence the appraisal process, few studies thus far have considered how contextual factors might play a role. Our study begins to address this gap. Notably, our findings may suggest that context, and specifically the device used, may shape the manner in which users assess threat severity. Although TTAT suggests that the severity of risk should generally have a positive effect on users' avoidance behavior, the results of Studies 2 and 3 did not support this proposition. Rather, the results suggest that the effect of risk severity on risk-avoidance behavior was contingent on the device used. In particular, whereas mobile and PC

users responded similarly to high-risk URLs, mobile users were significantly more likely than PC users to avoid lower-risk URLs. This result might suggest that PC users assessed the specific risk levels of the popup messages they observed—avoiding clicking messages with high risk levels more than messages with low risk levels—whereas mobile users perceived all messages as risky and thus avoided them to a similar extent.

This difference in risk-avoidance behavior between mobile users and PC users is also grounded in the work of Ghose et al. (2013), suggesting that because of the heightened search costs associated with mobile devices, mobile users simply click on links less often. Yet, this explanation cannot account for the fact that mobile and PC users' clicking behavior differed only in the presence of lower-risk links, whereas it was similar for higher-risk links. Moreover, it cannot account for the results of Study 1, in which risk-avoidance behavior was evaluated according to the types of URLs users accessed rather than by the frequency of access. Therefore, our findings suggest that the mechanism at play involves contextual differences beyond those related to search costs.

Summing up, our findings expand on TTAT and show that (1) the device of use is a contextual variable that influences users' appraisal of a risk, and (2) the effect of the severity of the risk on the tendency to avoid clicking on a link is moderated by the device used. With regard to our focus on phishing attacks, we suggest that users may respond differently to such attacks as a function of the device they use. If users' behavior in the presence of a risk is indeed affected by the device being used, then we are able to identify the device as a boundary condition in the context of security and privacy behavior, thereby offering a theoretical contribution to this literature.

6.3. Practical implications

This work has clear practical implications. In an age of increasing internet crime, particularly phishing attacks, our work adds to the growing understanding of risk-avoidance behavior. Furthermore, given the plethora of devices available to users, our findings advance the understanding of device-related behavioral differences. These novel insights can help cybersecurity companies design solutions that better fit the device being used and the desired user behavior. These companies should realize that risk-avoidance behavior may be device-dependent, implying that the security mechanisms that may prove to be most effective may be contingent on the device being used.

Our findings also have implications for web companies that seek to elicit various user behaviors that may involve risk appraisal processes (e.g., signing up for a new service, or providing contact or payment information). Specifically, when developing mobile and desktop apps, these companies should take into account mobile users' stronger tendency (as compared with PC users) to engage in risk-avoidant behavior, and incorporate these considerations into their user experience (UX) design. For example, for mobile users, it might be particularly important to provide cues indicative of trustworthiness, given that these users may be more prone to perceiving their environment as risky.

In terms of policy, understanding device usage and the impact on behavior outcomes, specifically in the context of security and privacy, can be useful for policymakers to better form regulations. Specifically, considering the evidence that users' perception of risk affects risk-avoidance behavior contingent on the device of use, policymakers should take into account these insights when creating policies and regulations. Such policies should focus on raising public awareness of the risks associated with using different devices, as well as creating and implementing regulation, instructions, and guidelines for companies to take different precautions with different devices. These insights regarding the importance of the device of use are especially valuable because detecting the type of device is not technologically challenging. Therefore, a viable way for reducing cybercrime may be take into account the device being used as a predictor of the likelihood of the user becoming a victim.

6.4. Limitations and future research directions

Naturally, this research has several limitations. First, as previously acknowledged, our capacity to make causal inferences on the basis of our field study (Study 1) is limited because of the endogenous nature of device selection. We addressed this limitation by carrying out two controlled studies in which devices were randomly assigned. Yet, controlled lab experiments introduce other limitations, such as external validity problems due to the unrealistic nature of the setting. To deal with these limitations, we invested a great deal of effort in creating a website that mimicked the participants' natural environment (for example, we chose a common task for AMT workers, i.e., an image tagging task). Nevertheless, our experimental setup cannot fully mimic a phishing attack encountered by a typical user outside the context of AMT.

Given these limitations, a viable avenue for future investigation would be to take a more granular approach to identifying the boundary conditions under which mobile users display higher levels of risk-avoidance behavior. Such an approach might entail, for example, investigating how cognitive processes of risk assessment differ between mobile and PC users. As mentioned, TTAT posits that risk appraisal, the process through which users evaluate a risk, is based on the users' perceived susceptibility and perceived severity of the threat. A future avenue of research would be to examine whether the device of use affects the former, the latter, or both. Such investigations may require the measurement of more subjective indicators of risk assessment.

Additionally, future research could propose and investigate different mechanisms that may mitigate the higher costs of assessing risk in mobile use. Another promising direction, aligned with the growing interest in artificial intelligence (AI) in online risk management, would be to examine how AI agents might compensate for users' reluctance to assess risks when using mobile devices. Such studies could explore the potential of AI to assist users in making safer decisions in situations where their own cognitive capacity to evaluate risks is compromised by the device they are using.

Eventually, both cognitive processes and observed behavior are likely to play pivotal roles in explaining the variance in the response of users to phishing attacks. By examining the interplay between these factors, future research could provide deeper insights into the role of device type in shaping risk-avoidance behaviors. The findings of this study, showing that mobile users are more risk-avoidant than PC users, particularly for lower-risk links, provide robust evidence in support of the view of the device as an important boundary condition in such explanations. Expanding this knowledge by investigating additional contextual and cognitive factors would not only refine our understanding of these behaviors, but could also inform the design of more effective security interventions tailored to different devices and use environments.

CRediT authorship contribution statement

Ilany-Tzur Naama: Writing – review & editing, Writing – original draft, Validation, Software, Project administration, Methodology, Investigation, Formal analysis, Conceptualization. **Fink Lior:** Writing – review & editing, Writing – original draft, Supervision, Methodology, Funding acquisition, Formal analysis, Conceptualization.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was supported by the Israeli Science Foundation (grant

604/18). We would also like to acknowledge Noa Benjo, Lihi Ohaion, Yuval Srur and Or Ben Zikry for their valuable contribution to this work.

References

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514. <https://doi.org/10.1126/science.aaa1465>
- Acquisti, A., & Grossklags, J. (2012). An online survey experiment on ambiguity and privacy. *Digiworld Economic Journal*, 88(4), 19–39. (<https://ideas.repec.org/a/ido/jtj/urnl/cs8801.html>).
- Berens, B. M., Mossano, M., & Volkamer, M. (2024). Taking 5 min protects you for 5 months: Evaluating an anti-phishing awareness video. *Computers Security*, 137, Article 103620. <https://doi.org/10.1016/j.cose.2023.103620>
- Birthriya, S. K., Ahlawat, P., & Jain, A. K. (2025). A comprehensive survey of social engineering attacks: Taxonomy of attacks, prevention, and mitigation strategies. *Journal of Applied Security Research*, 20(2), 244–292. <https://doi.org/10.1080/19361610.2024.2372986>
- Burch, G., & Hong, Y. (2014). What happens when word of mouth goes mobile? In *The Proceedings of the thirty fifth international conference on information systems*. Auckland, New Zealand. (<https://ssrn.com/abstract=2519931>).
- Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying phishing susceptibility for detection and behavior decisions. *Human Factors The Journal of the Human Factors and Ergonomics Society*, 58(8), 1158–1172. <https://doi.org/10.1177/0018720816665025>
- Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems*, 44, 380–407. <https://doi.org/10.17705/1CAIS.04422>
- Chae, M., & Kim, J. (2004). Do size and structure matter to mobile users? An empirical study of the effects of screen size, information structure, and task complexity on user activities with standard web phones. *Behavior Information Technology*, 23(3), 165–181. <https://doi.org/10.1080/01449290410001669923>
- Cozzarin, B. P., & Dimitrov, S. (2016). Mobile commerce and device specific perceived risk. *Electronic Commerce Research*, 16, 335–354.
- Davis, J. M., Agrawal, D., & Ogbanufe, O. (2025). Shaping extra-role security behaviors through employee-agent relations: A dual-channel motivational perspective. *International Journal of Information Management*, 80, Article 102833. <https://doi.org/10.1016/j.ijinfomgt.2024.102833>
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80. <https://doi.org/10.1287/isre.106>
- Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. *International Journal of Information Management*, 50, 261–272. <https://doi.org/10.1016/j.ijinfomgt.2019.05.010>
- Donalds, C., & Osei-Bryson, K. M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, 51, Article 102056. <https://doi.org/10.1016/j.ijinfomgt.2019.102056>
- FBI. (2025). Internet Crime Report 2024, *International crime complaint center in the federal bureau of investigation*. Retrieved from (<https://www.ic3.gov/AnnualReport/Report%2024/IC3Report.pdf>).
- Fink, L. (2022). Why and how online experiments can benefit information systems research. *Journal of the Association for Information Systems*, 23(6), 1333–1346.
- Fink, L., & Papismedov, D. (2023). On the same page? What users benefit from a desktop view on mobile devices. *Information Systems Research*, 34(2), 423–441. <https://doi.org/10.1287/isre.2022.1140>
- Frederick, S. (2005). Cognitive reflection and decision making. *Journal of Economic Perspectives*, 19(4), 25–42. <https://doi.org/10.1257/089533005775196732>
- Furner, C. P., & Zinko, R. A. (2017). The influence of information overload on the development of trust and purchase intention based on online product reviews in a mobile vs. web environment: An empirical investigation. *Electronic Markets*, 27(3), 211–224. <https://doi.org/10.1007/s12525-016-0233-2>
- Gallo, L., Gentile, D., Ruggiero, S., Botta, A., & Ventre, G. (2024). The human factor in phishing: Collecting and analyzing user behavior when reading emails. *Computers Security*, 139, Article 103671.
- Gerpott, T. J., & Thomas, S. (2014). Empirical research on mobile internet usage: A meta-analysis of the literature. *Telecommunications Policy*, 38(3), 291–310. <https://doi.org/10.1016/j.telpol.2013.10.003>
- Ghose, A. (2017). *Tap: unlocking the mobile economy*. Cambridge, MA: MIT Press.
- Ghose, A., Goldfarb, A., & Sang, P. H. (2013). How is the mobile internet different? Search costs and local activities. *Information Systems Research*, 24(3), 613–631. <https://doi.org/10.1287/isre.1120.0453>
- Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defense mechanisms: State of art and open research challenges. *Computers Security*, 73, 519–544. <https://doi.org/10.1016/j.cose.2017.12.006>
- Goenka, R., Chawla, M., & Tiwari, N. (2024). A comprehensive survey of phishing: Mediums, intended targets, attack and defence techniques and a novel taxonomy. *International Journal of Information Security*, 23(2), 819–848. (<https://link.springer.com/article/10.1007/s10207-023-00768-x>).
- Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: State of the art and future challenges. *Neural Computing and Applications*, 28, 3629–3654. <https://doi.org/10.1007/s00521-016-2275-y>
- Hansen, Jared M., George Saridakis, and Vladlena Benson. "Risk, trust, and the interaction of perceived ease of use and behavioral control in predicting consumers' use of social media for transactions." *Computers in human behavior* 80 (2018): 197–206.
- Ilany-Tzur, N., & Fink, L. (2022). How is mobile task performance different? The case of information processing without information search. *Behaviour Information Technology*, 42(15), 2572–2587. <https://doi.org/10.1080/0144929X.2022.2134824>
- Jakobsson, M., & Myers, S. (2006). Eds. *Phishing and countermeasures: Understanding the increasing problem of electronic identity theft*. Hoboken, NJ: Wiley-Inter Science, a John Wiley & Sons Inc. Publication.
- Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, 34(2), 597–626. <https://doi.org/10.1080/07421222.2017.1334499>
- Kahneman, D., & Tversky, A. (2000). Choices, values, and frames. *American Psychologist*, 39(4), 341–350. <https://doi.org/10.1037/0003-066X.39.4.341>
- Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, 47(2), 263–291. https://doi.org/10.1142/9789814417358_0006
- Lee, D., Moon, J., Kim, Y. J., & Mun, Y. Y. (2015). Antecedents and consequences of mobile phone usability: Linking simplicity and interactivity to satisfaction, trust, and brand loyalty. *Information Management*, 52(3), 295–304. <https://doi.org/10.1016/j.im.2014.12.001>
- Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45, 13–24.
- Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 33(1), 71–90. <https://doi.org/10.2307/20650279>
- Liu, F., Ngai, E., & Ju, X. (2019). Understanding mobile health service use: An investigation of routine and emergency use intentions. *International Journal of Information Management*, 45, 107–117. <https://doi.org/10.1016/j.ijinfomgt.2018.09.004>
- Levi-Bliech, M., Kurtser, P., Pliskin, N., & Fink, L. (2019). Mobile apps and employee behavior: An empirical investigation of the implementation of a fleet-management app. *International Journal of Information Management*, 49, 355–365. <https://doi.org/10.1016/j.ijinfomgt.2019.07.006>
- Maniar, N., Bennett, E., Hand, S., & Allan, G. (2008). The effect of mobile phone screen size on video-based learning. *Journal of Software*, 3(4), 51–61.
- Ou, C. X., Zhang, X., Angelopoulos, S., Davison, R. M., & Janse, N. (2022). Security breaches and organization response strategy: Exploring consumers' threat and coping appraisals. *International Journal of Information Management*, 65, Article 102498. <https://doi.org/10.1016/j.ijinfomgt.2022.102498>
- Owen, M., Flowerday, S. V., & van der Schyff, K. (2024). Optimism bias in susceptibility to phishing attacks: An empirical study. *Information Computer Security*, 32(5), 656–675. <https://doi.org/10.1108/ICS-02-2023-0023>
- Pavlou, P. A., Lie, T., & Dimoka, A. (2007 November). An integrative model of mobile commerce adoption. In *The Conference on Information Systems and Technology (CIST/INFORMS)*. Seattle, WA, USA. (<https://ssrn.com/abstract=2380676>) (Seattle, WA, USA).
- Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly*, 25(4), 977–988. (<https://www.jstor.org/stable/41409969>).
- Piccoli, G., & Ott, M. (2014). Impact of mobility and timing on user-generated content. *MIS Quarterly Executive*, 13(3), 147–157.
- Pienta, D., Thatcher, J.B. and Johnston, A.C. (2018 December). A taxonomy of phishing: Attack types spanning economic, temporal, breadth, and target boundaries. In *Proceedings of the WISP 2018 pre-ICIS workshop on information security and privacy (SIGSEC)*. San Francisco, CA, USA. Retrieved from (<https://aisel.aisnet.org/wisp2018/19/>).
- Pousttchi, K., Tilsen, D., Lyytinen, K., & Hufenbach, Y. (2015). Introduction to the special issue on mobile commerce: Mobile commerce research yesterday, today, tomorrow—What remains to be done? *International Journal of Electronic Commerce*, 19(4), 1–20. <https://doi.org/10.1080/10864415.2015.1029351>
- Rabin, M., & Thaler, R. H. (2001). Risk aversion. *Journal of Economic Perspectives*, 15(1), 219–232. <https://doi.org/10.1257/jep.15.1.219>
- Raphaelli, O., Goldstein, A., & Fink, L. (2017). Analyzing online consumer behavior in mobile and PC devices: A novel web usage mining approach. *Electronic Commerce Research and Applications*, 26, 1–12. <https://doi.org/10.1016/j.elerap.2017.09.003>
- Ravula, P., Bhatnagar, A., & Jha, S. (2024). Comparing the effectiveness of recommendation agents across devices. *International Journal of Information Management*, 76, Article 102758. <https://doi.org/10.1016/j.ijinfomgt.2024.102758>
- Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 989–1016. <https://doi.org/10.2307/41409970>
- Sweeney, S., & Crestani, F. (2006). Effective search results summary size and device screen size: Is there a relationship? *Information Processing Management*, 42(4), 1056–1074. <https://doi.org/10.1016/j.ipm.2005.06.007>
- Thakur, K., Qiu, M., Gai, K. and Ali, M.L. (2015 November). An investigation on cyber security threats and security models. In *Proceedings of the IEEE second international conference on cyber security and cloud computing*, New York, NY, 307–311. <https://doi.org/10.1109/CSCloud.2015.71>
- Verkijika, S. F. (2019). If you know what to do, will you take action to avoid mobile phishing attacks: Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior*, 101, 286–296. <https://doi.org/10.1016/j.chb.2019.07.034>
- Wang, J., Li, Y., & Rao, H. R. (2016). Overconfidence in phishing email detection. *Journal of the Association for Information Systems*, 17(11), 759–783. <https://doi.org/10.17705/1JAIS.00442>
- Wong, L. W., Lee, V. H., Tan, G. W. H., Ooi, K. B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes:

- Building supply chain capabilities. *International Journal of Information Management*, 66, Article 102520.
- Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research note—Influence techniques in phishing attacks: An examination of vulnerability and resistance. *Information Systems Research*, 25(2), 385–400. <https://doi.org/10.1287/isre.2014.0522>
- Xu, K., Chan, J., Ghose, A., & Han, S. P. (2016). Battle of the channels: The impact of tablets on digital commerce. *Management Science*, 63(5), 1469–1492. <https://doi.org/10.1287/mnsc.2015.2406>
- Yang, Q., Pang, C., Liu, L., Yen, D. C., & Tarn, J. M. (2015). Exploring consumer perceived risk and trust for online payments: An empirical study in China's younger generation. *Computers in Human Behavior*, 50, 9–24. <https://doi.org/10.1016/j.chb.2015.03.058>
- Zahedi, F. M., Chen, Y., & Zhao, H. (2024). Ontology-based intelligent interface personalization for protection against phishing attacks. *Information Systems Research*, 35(3), 1463–1478. <https://doi.org/10.1287/isre.2021.0065>