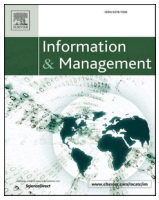
Information & Management 60 (2023) 103860

Contents lists available at ScienceDirect

Information & Management

journal homepage: www.elsevier.com/locate/im



How "What you think you know about cybersecurity" can help users make more secure decisions

Amir Fard Bahreini [a,*], Hasan Cavusoglu [b], Ronald T. Cenfetelli [b]

[a] Department of Information Technology and Supply Chain Management, College of Business and Economics, University of Wisconsin–Whitewater, 800W Main St, Whitewater, WI 53190, United States
Accounting & Information Systems Division, Sauder School of Business, University of British Columbia, 2053 Main Mall, Vancouver, BC V6T 1Z2, Canada

ARTICLE INFO

Keywords:
Information security
Theory of bounded rationality
Objective security knowledge
Subjective security knowledge
Default settings

ABSTRACT

The increasing use of information technology artifacts in daily life makes security a shared responsibility of both users and companies. In recent years, increasing a user's objective (i.e., actual) security knowledge and providing applications with more secure default settings appear among the most ubiquitous tools companies use to broaden their efforts to help users make more secure decisions. Examining both solutions matters because they are widely used, cost effective, and understood by many security practitioners. Additionally, default settings and users' objective knowledge provide anchors for decision-making. However, human errors and insecure default settings are increasing and raising further questions about the efficacy of such efforts. Using the theory of bounded rationality, we investigated the role of objective, subjective (i.e., self-assessed) security knowledge, and default settings security level on the overall decision security. We found that objective security knowledge can lead to secure decisions when paired with high subjective security knowledge. In the absence of the latter, objective security knowledge is unable to lead to better security decisions. Furthermore, subjective security knowledge reduces the extent to which users fully accept default security settings, thereby mitigating bias toward insecure default settings.

1. Introduction

People play a critical role in cybersecurity [1] but are generally considered the weakest link because of their propensity for errors in security-related decisions [1–3]. This was starkly evident in the 2022 Verizon Data Breach report, showing the involvement of one or more employees in 82% of security breaches, including phishing, ransomware, credential theft, or errors [4]. In that same year, IBM reported that poor human decisions were the primary cause of 21% of breaches, with each attack costing an average of 4.35 million USD [5]. As the global economy transitions toward a post-pandemic era and more activities transition to online venues, the number of decisions that individuals—particularly employees—must make is increasing. Thus, helping individuals make decisions that include a high level of security is a priority for many organizations. Currently, two solutions appear to be feasible, ubiquitous, and cost-effective: increasing the objective security knowledge of individuals and implementing secure default settings [3].

In the judgment and decision-making literature, knowledge historically comprises objective knowledge (i.e., what a person actually knows) and subjective knowledge (i.e., what a person thinks he or she knows) [6]. Between the two, objective security knowledge has been the sole focus of most, if not all, security training in the workplace and public forums [7–10]. The idea of providing users training with an objective knowledge focus is simple: the greater one's objective security knowledge is, the more secure a user's security decisions will be. This impact is substantial; objective knowledge influences various facets of decision-making, including information search and processing [11–14]. Furthermore, it impacts decision quality [15]. In a simple example, an individual who secures a higher level of objective knowledge follows it with a search for information sufficiency, processes the information more deliberately, and ultimately makes a better decision. In the past decade, reports have indicated that the average user understands common security-related terms, such as "computer virus" and "firewall," and is aware of recommended practices [1,16]. Yet, despite such encouraging reports and the expansion of security training programs in organizations and on public platforms (e.g., NSA guidelines for home users, GetCyberSafe Canada), the number of human errors continues to rise. For example, in a multinational survey, approximately 90% of respondents knew the criteria for

* Corresponding author.
E-mail address: fardbaha@uww.edu (A. Fard Bahreini).

https://doi.org/10.1016/j.im.2023.103860
Received 16 July 2022; Received in revised form 5 September 2023; Accepted 6 September 2023
Available online 9 September 2023

strong passwords and the risk of using the same password for multiple accounts [17]. This matter also relates to the "knowing-doing gap" [18], in which there appears to be a disconnect between what employees know and their commitment to security countermeasures. This phenomenon notes that, despite increased investments and a heavy focus on technical facets of cybersecurity, there has not been an adequate focus on behavioral factors [18,19]. Nevertheless, human errors still pose the most significant security issue [20,21]. Human errors in cybersecurity are threats a company faces from individuals (mostly employees) without intentional malice. For example, Verizon has consistently reported that an average of 80% of data breaches within their samples are attributable to compromised, weak, and reused passwords [4,22]. These observations led us to question whether the role of objective security knowledge is more complicated than it appears. Is a lack of investigation into the role of subjective knowledge depriving us of a clear understanding of the role of objective security knowledge? Indeed, theorizing and support exist for subjective knowledge—a form of self-referential belief—impacting decision-making in various ways, such as pushing individuals to make their own decisions and relying less on external information [6,16,24,25]. Consequently, here, we investigate the influence of objective and subjective security knowledge on security decision-making.

The second ubiquitous security solution is using secure default settings [3]. In the context of cybersecurity, default settings are the initial state of security options presented to users, another tool at the disposal of companies and platform owners. In information security, default settings figure in many user decisions when users interact with information technology (IT) artifacts. For instance, during account setup, a user receives several security options (e.g., two-factor authentication [2FA], login alert) with an initial state of being "on" or "off." Both application software and system software (operating system and utilities), on smartphones, PCs, and most websites include security options (i.e., settings) with a default state. Yet, despite the ubiquitous use of default security settings, not all are secure. Because of status quo bias [26] and the reluctance of users to change defaults, companies using default settings to enhance users' security might appear reasonable. However, not all platforms offer users the most secure options. In the mobile app market, with nearly three million applications in the Google Play and Apple App stores, various default security levels exist even within the same category of apps [27]. Some apps have more secure default settings ("high-level security"). Although Facebook offers several secure defaults, some defaults are less secure. For example, Facebook does not automatically turn on the login alert from a new device or enable 2FA (at this writing). Furthermore, the number of malicious apps has risen [28–30]. For example, the first three months of 2020 saw more than 29,000 malicious Android apps identified [31]. In 2022, two million device owners downloaded 35 apps with malicious features [32]. These apps use a variety of approaches to access users' data, including in-app ads and less secure default settings. Accordingly, they most often have insecure defaults ("low-level security"). The state of the app marketplace led us to wonder whether low-security defaults influence users to the same degree as high-level security defaults, and what prevents or promotes users' blindly relying on the defaults when selecting security settings.

Our formal research questions are:

1. How influential is objective security knowledge in users' security decision-making?
2. What differences exist in the extent to which low-level and high-level security default settings influence users?
3. How does subjective security knowledge impact the utilization of objective security knowledge?
4. How does subjective security knowledge prevent users from blindly accepting default settings?

Accordingly, this study aimed to assess the roles of users' objective security knowledge, default security settings, and subjective security knowledge in their security decision-making. Furthermore, we examined the relationship among these three constructs in the security decision-making process. To answer these questions, we turned to the theory of bounded rationality [33–35], which provides a comprehensive foundation for knowledge and environmental factors (e.g., default settings) that other judgment and decision-making studies have used and expanded [6,13,23,36]. We aimed to create a study that measured all three of these main constructs while controlling for factors that could affect users' security decision-making (e.g., IT experience, self-efficacy). To that end, we conducted a three-day field study for which we recruited 95 users via Prolific.co (an online academic-research recruitment platform). We began by developing a questionnaire to accurately measure personal objective security knowledge. Then, to capture the actual security level of a security-related decision, we used the actual (observed) security level of settings that users selected within the app that we specifically designed and developed for this study. The app was designed to work on both IOS and Android devices and was deployed in the Google Play and Apple App stores. The study participants downloaded the app from one of the app stores, used it, and assessed its design and functionality.

We found that objective security knowledge resulted in more secure decisions when combined with high-level subjective security knowledge. However, in the absence of subjective knowledge, objective security knowledge cannot lead to better security decisions. Furthermore, subjective security knowledge reduces the degree to which users unquestioningly accept default security settings, helping them avoid the pitfall of insecure defaults.

2. Theoretical development

2.1. Bounded rationality in information security

Historically, the information security literature has mostly drawn on theories that assume users are rational [37]. Protection motivation theory [38] and technology threat avoidance theory [39] have been among the most dominant frameworks in the individual users' security literature. However, "[People] are predictably irrational," notes Ariely [40]. Studies have begun to recognize that human beings are not rational actors, even when the theory of bounded rationality is not the explicit basis of research models. Many of these studies focus on privacy, information disclosure, and how such factors as emotions, herd behavior, and saliency impact users' disclosures, with a few focusing on security precautions behavior [41–48]. The folk security models, which attempt to explain how users categorize various security threats and reveal individual user limitations, also discuss irrationality [47]. Our study attempts to extend this line of information system (IS) security research by using the theory of bounded rationality and to examine the interplay among and impact of three constructs on a user's decision security level: objective security knowledge, subjective security knowledge, and default settings' security level.

2.2. Theory of bounded rationality

"Any particular concrete behavior is the resultant of a large number of premises there will be premises about the state of the environment based directly on perception, premises representing beliefs and knowledge.[49], p. 274

The theory of bounded rationality is a descriptive decision theory developed by Simon [33–35,49]. The most important assumption in this theory is the possibility of irrationality. It simply states that individuals are prone to cognitive limitations in any decision and may not act rationally at all times [35]. At the center of bounded rationality are knowledge and its limitations. Accordingly, decision-makers make their decisions on the basis of knowledge they may or may not have and the state of the decision's environment [33,50]. This premise allowed researchers to examine how people actually make decisions rather than

how they ought to make decisions (i.e., normative models). Finally, the theory is prevalent in domains where many individuals are not experts on a subject (such as consumer behavior) and it aims to explain various decisions and deviations from normative decision models [51].

Many researchers began exploring human behavior using the underlying assumptions of bounded rationality (i.e., the possibility of irrationality). Subsequently, the judgment and decision-making domain primarily categorized knowledge as objective and subjective [6,13,14,23]. We used these two constructs to represent the knowledge and perception of knowledge that Simon discussed. Finally, we chose default settings as a representation of the state of the environment. Default settings or choices are the single common ubiquitous environmental factors across most economic decisions, including security choices [26].

Bounded rationality provides a rich framework for understanding how these three constructs interact and influence decisions. Objective knowledge is integral because people often rely on their actual knowledge to make decisions [6]. Default settings often lead to status quo bias in decisions [26]. Finally, subjective knowledge, a form of self-referential belief, impacts decision-making in various ways, two of which are relevant to this study context: *its relationship with objective knowledge* and *its impact on one's willingness to make decisions*. More specifically, self-referential thoughts appear to mediate actual knowledge in decision-making [24,25]. Despite what one actually knows, self-referential thoughts can help one reach optimal solutions to problems. Furthermore, subjective knowledge is proposed to increase one's willingness to act [6,13,23].

2.3. Objective security knowledge

2.3.1. Construct explication and background

Objective security knowledge is one's actual security knowledge. Drawing on definitions of various relevant constructs (e.g., IT security knowledge, cybersecurity knowledge), we developed a comprehensive definition of objective security knowledge in this study. First, Aggarwal et al. [52, p. 131] define IT security knowledge as the "awareness of common security threats and available defense mechanisms." Additionally, the existing cybersecurity practice commonly notes that threats and defense mechanisms can arise from human and technical sources [53]. An awareness of information security includes a multipronged understanding of its mechanisms: confidentiality (i.e., only allowing authorized users to access and modify data), availability (i.e., ensuring authorized users can access data whenever they require it), and integrity (i.e., ensuring the data is accurate, reliable, and not tempered with). Thus, we define objective security knowledge as:

An awareness of common technical and human security threats and available defense mechanisms to protect confidentiality, integrity, and data availability.

The research on objective knowledge's role is much greater than that on the role of subjective knowledge and has historically garnered more academic interest. Specifically, prior research has assessed the influence of objective knowledge on information processing [11,12], information searches [13,14], and decision quality [15]. In particular, objective knowledge increases the use of newly acquired information [54] and expands search efforts to add new information regarding the products of interest [11]. This is an interesting contrast to the effect of subjective knowledge on search efforts, in which users relied less on external search and more on memory-based information [13,55,56]. Lusardi and Mitchell [15] reported that greater objective financial knowledge leads to better financial planning and more retirement wealth.

2.3.2. Background in information security literature

The security literature has also investigated objective security knowledge. Higher-level cybersecurity knowledge in network operations and information security helps increase the accuracy of detecting malicious events and decreases the false classification of benign events [57]. Higher degrees of information security knowledge suggest better performance in cyber incident detection [58]. For example, the IS security literature states that information security policy (ISP) knowledge and awareness of security threats and their potential consequences are strong determinants for encouraging compliance with organizations' information security rules [59,60].

Although some studies used a knowledge questionnaire [52,61], others used participants' self-reports as a proxy for actual knowledge [62]. These studies (such as [59]) use a self-reported Likert scale as a proxy to measure ISP knowledge and not an actual knowledge quiz.

2.4. Subjective security knowledge

2.4.1. Construct explication and background

Subjective security knowledge is one's security knowledge self-assessment. In addition to the security literature, the construct has been a focal point of interest in judgment, decision-making, and marketing literature for years [6,11,13].

Conceptually, subjective knowledge is a perceptual construct (i.e., self-referred thought). It differs from other perceptual constructs in concept and operationalization. For example, belief constructs, such as perceived self-efficacy, refer to one's belief in the agentive capability one can have, based on a given level of attainment. Thus, it includes both the strength and the certainty of one's belief in their capabilities. On the other hand, subjective knowledge only encompasses the strength of one's belief but does not specify anything about certainty [24]. Busey et al. [63] make this distinction clearer. Self-efficacy is *a priori* to tasks and refers to the general self-perception that one has in a given domain, without actually knowing the context of that domain (e.g., before or [in our experiment] without a knowledge-based quiz that reveals boundaries and context). However, self-assessment of knowledge after having learned its actual context shapes subjective knowledge *a posteriori* to tasks [63,64] (e.g., following a knowledge-based quiz that reveals the boundaries and context). This temporal property arose in discussions supporting early knowledge-focused studies, showing that self-efficacy is an antecedent of and a control variable for subjective knowledge [11,55]. Furthermore, the operationalization of these constructs also emphasizes this subtle yet crucial difference. Using a Likert scale measuring self-efficacy, participants directly answer what they think they know about their knowledge or skill in a topic area [64]. Conversely, they assess subjective knowledge based on individual reviews of their performance in a given quiz [6]. Consequently, subjective knowledge is retrospective and self-efficacy is prospective [63,64].

With respect to self-efficacy in information security, incentive designs in car digital assistants that enhance the user's self-efficacy reduces those users' psychological ownership of data and enhance their willingness to share it [65]. Self-efficacy is also a predictor of workgroup collective efficacy and security knowledge coordination. However, the authors did not find support for a significant relationship between efficacy and workgroup information security effectiveness (how effectively the group follows best practices against security threats) or an objective measure of group performance [66]. Furthermore, self-efficacy was a positive and significant predictor of behavioral intent to use anti-spyware software, a finding confirmed in the context of home users' intentions of secure behavior [1]. Finally, self-efficacy is also a predictor of perceived avoidability in technology avoidance theory [39] and one of the predictors of individuals' compliance with information security policies [67]. Following prior studies, we used self-efficacy as an antecedent for subjective security knowledge.

Concerning its antecedents, in addition to self-efficacy, one's prior experience and expertise influence subjective knowledge [12]. Prior studies highlight the various roles that subjective knowledge can play. Higher subjective knowledge increases individuals' reliance on information previously stored in their memory [54]; it leads individuals to search for less information in a database before answering questions on birth control [55] and search for less external information when selecting a VCR [13]. Subjective knowledge causes individuals to put

more money into emergency savings to ultimately help their future financial well-being [56] and may lead to more risky investments that may or may not pay off [68].

2.4.2. Background in information security literature

Over the years, there has been an increased effort to examine perceptions and beliefs in information security literature. However, to the best of our knowledge, these efforts have not examined the relationship between subjective security knowledge—*a posteriori* perception, as this paper distinguishes it—and actual security decisions. Starting with general belief studies, researchers have delved into the role of users' perceptions of security and privacy [69–72]. For example, in choosing between biometric authentication methods, users prefer methods they perceive to be more secure [73]. In selecting passwords, users apply methods that they perceive as secure [74,75]. In the context of team security effectiveness, authors have shown that group self-efficacy mediates individual self-efficacy [66]. Although the existing literature studies the discrepancy between subjective knowledge and objective knowledge in security and privacy [61,64,76], it has thoroughly investigated subjective security knowledge.

From the perspective of including subjective security assessments, Wang et al. [64] is the closest study to ours. Like us, they discuss the distinction between retrospective and prospective self-assessment. However, they do not examine subjective knowledge but rather evaluate whether the subjective assessment of participants' performance (decision) is a good predictor of phishing email detection accuracy. In that study, 600 participants received fifteen email screenshots and asked to determine if the email was legitimate or malicious. Subsequently, their subjective performance assessment was measured. The results failed to establish a significant correlation between subjective performance assessment and phishing email detection accuracy [64]. However, the authors did not assess users' objective or subjective security knowledge because their sole focus was on phishing-detection performance.

2.5. Default settings' security level

2.5.1. Construct explication and background

We define default settings' security level as *the degree to which the overall initial default settings are secure*. We dissect this construct, first, by declaring that default settings may include several options, such as 2FA, login alert from a new device, automatic update, cookies, and location access. This is also an area in which information security differs from traditional economic decisions and other fields that have examined defaults. Specifically, in non-security contexts, individuals often face one choice at a time. For example, in a retirement plan study, participants could accept the plan or not. However, in information security, settings typically provide several choices. For example, the user must accept or change the default for each of the options (e.g., login alert, cookies). This creates a distinction between the former context and many other economic contexts in which it is not just one choice that matters but rather the amalgamation of choices. In other words, to consider a decision secure, a person makes several secure choices. For example, security settings are not considered secure if the person has made one secure choice (e.g., login alert) and several insecure choices (e.g., ads). Thus, the overall setting quality operates on a security continuum rather than a dichotomous secure/insecure model.

The second part of this definition is the security level of the default settings. Because a particular selection of each setting implies different security, a degree of objective variability always applies to how well or poorly the security of default settings can protect against online threats. For instance, if developer A has turned on "2FA" and "login alert from a new device" and developer B has only turned on "2FA," developer A has presented default settings with a higher security level than developer B. Hence, we label the construct as the default settings' security level.

Outside of a security context, the literature has reported the role of the default option largely involving one choice. Samuelson and Zeckhauser [26] are among the first to provide evidence for the role of the default option. Given a set of alternatives, one of which is labeled as the default (i.e., status quo), people will more likely choose that option. The potential error from this process, labeled status quo bias, subsequently generated significant interest from various fields. Many studies following that seminal paper support the presence of a status quo bias. For example, health professionals in Taiwan resist accepting new cloud-based technology and are prone to status quo bias [77]. In another example, when a select number of employees of an organization implementing new Office Plus software was surveyed, the authors discovered that participants would rather use the existing software and resisted the adoption of new software, despite its superiority [78].

2.5.2. Background in information security literature

Although information security involves confidentiality, integrity, and availability of data, prior studies related to default settings were interested in default settings related to data confidentiality (i.e., privacy) [72,76,79–82]. This focus is attributable to the sensitivity of privacy and the increasing public interest in privacy after the Edward Snowden Facebook data leaks. The privacy literature on default settings mostly focused on the design of default settings in personal information disclosure on such social network sites as Facebook [83,84]. For instance, in a laboratory experiment using a birthday app that connects to Facebook, when default settings are relevant to users and aligned with the context of the information request (e.g., information about one's birthday), participants are more likely to share that specific personal information [85]. Following this trend, several studies have attempted to provide proof of concept for smart default privacy settings, which are default settings that use machine-learning techniques to generate personalized privacy settings that capture users' preferences and the app context [86,87].

Discussion of the relevance and potential importance of default settings has also occurred to a lesser degree. For example, prior studies have commented that individuals are likely to retain default choices [3]. The consumer behavior literature explicitly inspired that statement, describing how users often buy additional items when firms automatically add them to their purchase basket [88]. However, as this paper has defined it, the security level of many users' decisions is not a dichotomous construct. Instead, it is a continuum with varying levels of security (insecurity), and security settings often involve multiple options. Depending on each option's selection, the aggregate security level of security settings can vary across users. In cases in which the decision consists of multiple choices, the role of defaults remains unclear. Do users simply accept the default settings they receive (either high-level or low-level security) without any changes? Or do they use defaults as anchors and then make their own adjustments? There is a subtle yet vital difference between these two possibilities. The former suggests that users will accept the default status of all the individual options they see without any changes—the prevailing assumption in the security literature [3]. However, the latter suggests that users use the defaults as an anchor from which to make additional changes. Our study aimed to shed light on how users interact with the defaults in the context of the security of an actual app.

3. Hypothesis development

3.1. Objective security knowledge → user's decision security level

Objective knowledge is an important direct input for decision-making [6]. In marketing, higher objective knowledge affects the number of product attributes individuals assess when making decisions and ultimately enabling them to make better decisions [6,12]. For instance, Brucks [11] shows that individuals with higher objective

knowledge review more relevant product attributes in purchase decisions. Various domains also link objective knowledge to better performance quality. For instance, empirical IT knowledge positively influences managers' intention to champion IT in their organizations [89]. Furthermore, objective knowledge improves the quality of financial decisions [15]. IS security literature argues that higher objective security knowledge increases cyber incident detection and network security compliance [57–59]. Accordingly, in the context of personal information security, we posit:

H1: *Higher levels of objective security knowledge will increase the user's decision security level.*

3.2. Default settings' security level → user's decision security level

A normative approach would suggest that the default does not matter, and individuals will choose the optimal level of security for their needs by maximizing the utility of their decisions. However, the theory of bounded rationality proposes a different perspective, namely, that the default option is set as an anchor from which users will make a decision. Tversky and Kahneman [90] introduced the anchoring effect, which refers to circumstances in which individuals make a decision on the basis of an initial anchor. For example, individuals tend to disclose more information if defaults promote this type of data sharing [83,84]. Thus, a default option is an external anchor that decision-makers can use. Based on the theory of bounded rationality, if an option can make decision-making easier, individuals will use it. Accordingly, if an anchor is present, individuals assess alternatives relative to this anchor, influencing their ultimate decision.

People use external anchors in a two-step process: comparative assessment followed by absolute judgment [92]. In the first step, the individual compares the alternative option to the default option. Dhingra et al. [93] label this particular effect as the *default pull*. Simply put, when presented with several alternatives, where one is set as the default, the decision regarding which is the best alternative will become deciding whether the individual prefers the default alternative over others. Many users will prefer the default. For instance, if the default turns on a 2FA option, the user will ask, "Do I prefer to keep 2FA or not?" An absolute judgment follows when users decide whether 2FA is an effective option. Default pull appears in such decision-making contexts as medicine and health care [93].

Although many prior studies in other domains have explored whether people keep or change an option (i.e., a dichotomous outcome), information security finds understanding the degree to which people make changes to security settings to be critical on the basis of the defaults they receive. As noted, the security level of user decisions falls on a continuum of smaller decisions. Security settings selection is a helpful example of where the degree of change matters. For instance, someone facing an insecure default may change the settings, but the choices may still be less secure because of the anchoring effect of that low-level default. Based on the same effect, people receiving high-level security defaults from which to choose will likely make more secure decisions. This could result from a lack of knowledge, preventing individuals from making informed decisions, or a desire to avoid effort in decision-making.

Consequently, default settings act as a double-edged sword. If preselected default settings occupy a higher security level, then users are likely to select the options at a higher security level. If preselected defaults occupy a lower security level, then users are likely to select the options at a lower security level. Accordingly, we propose that these default pulls also emerge in information security. Specifically, we postulate:

H2: *High-level security defaults increase the user's decision security level, whereas low-level security defaults lead to a decrease in the user's decision security level.*

3.3. Objective security knowledge → subjective security knowledge

Subjective knowledge is a function of objective knowledge [11,13,23]. As Russo and Shoemaker [94] argue, subjective knowledge helps individuals understand the scope and limitations of their knowledge. This self-assessment improves as one's objective knowledge increases. Essentially, as individuals gain more objective knowledge in a given domain, they become more cognizant of their actual abilities and limitations, causing higher-level subjective knowledge. Applying this argument to information security, we propose that the same relationship holds. As users increase their knowledge of threats and defense mechanisms that protect their information security, they better understand their capabilities. Accordingly, we expect this relationship to be positive. Thus, we postulate:

H3: *As objective security knowledge increases, subjective security knowledge increases.*

3.4. Subjective security knowledge → user's decision security level

Subjective knowledge helps people understand the scope and limitations of their objective knowledge, or "metaknowledge" [94]. Higher levels of subjective knowledge are associated with greater proactivity in making various decisions and engagement in the decision-making process [2,15]. For example, some financial literature suggests that subjective knowledge will lead to better investment strategies and financial well-being [56,95]. Subjective security knowledge increases reliance on memory-based information [56]. In IS security, users tend to act on thoughts they perceive as secure to set their passwords [74,75] and follow security precautions [46]. We argue that this also applies to information security decision-making. Increased awareness will help users identify the scope of their knowledge and allow them to make more secure decisions. Consequently, we postulate:

H4: *Higher levels of subjective security knowledge will increase the user's decision security level.*

Fig. 1 displays the complete theoretical model.

4. Methodology

4.1. Capturing users' actual security decisions

To increase the study's ecological validity and improve the measurement of the security decision construct that prior work [6,96] recommends, we captured users' actual security decisions using a mobile app that we developed for this study (sample screenshots appear in Fig. 2). This enabled us to observe first-hand a user's behavior, such as their chosen security settings. The app offered location-based services, news, and social media updates about the university. It was a real app, available through two major mobile app stores at the time of the study. Additionally, because the app required installation on participants' devices, it created a realistic scenario in which users' decisions were relevant. We designed sixteen dichotomous security options with defaults (i.e., "on" or "off") for the app based on security options available in existing apps and platforms. As noted, many studies have focused on confidentiality (i.e., privacy).

However, our goal was to examine all three facets of information security. Accordingly, we included those focusing on confidentiality, availability, and integrity of data to the extent that each was relevant to the context of the app. To measure the user's decision security level, we scored each final option the user selected relative to a predefined security-level point. Each secure (insecure) option received one (zero) point. For example, if the user turned on "Login alert," the decision counted as a secure decision, and the user received one point; otherwise, the score was zero. Therefore, the total points for the user's decision security level ranged from zero to sixteen (see Table 1 for the point system structure).

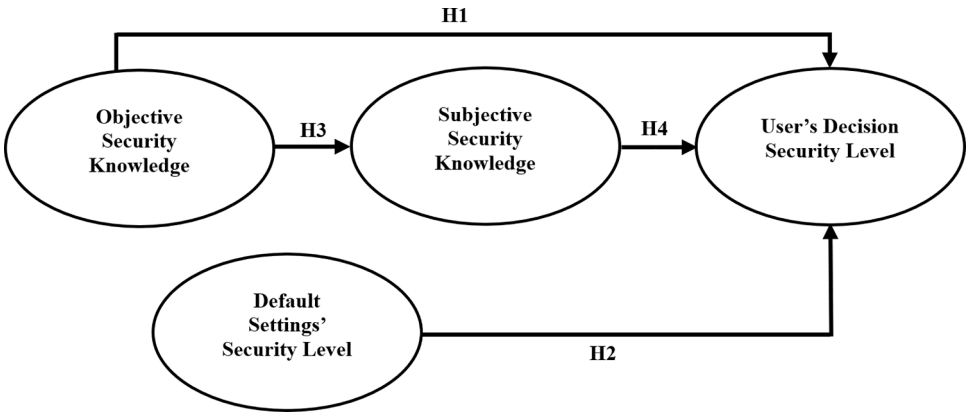


Fig. 1. Theoretical Model.

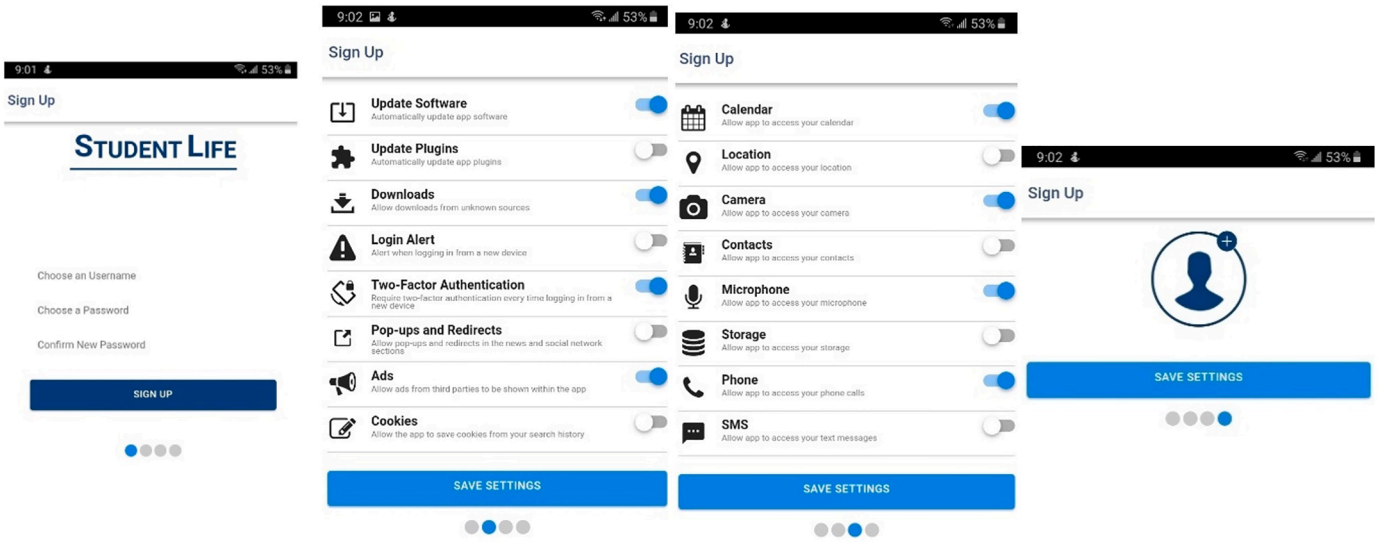


Fig. 2. Mobile App.

4.2. Study procedure

The data collection took place over three days. Based on two rounds of pilot studies, we did not disclose the study's primary intentions to the participants until after the study concluded to avoid possible priming effects from revealing the study's focus (i.e., information security). To further prevent the priming effect, we added a ten-question quiz examining the participants' knowledge of the app design process in addition to the twenty-question objective security knowledge quiz. We recruited the subjects using the premise that they would participate in an app-testing study in which they would assess the functionality and design of a newly developed mobile app. They received a flat compensation fee for their time commitment to completing the study. We chose this approach to capture users in a natural setting and avoid tying study compensation to security decisions. At the end of the study, we also encouraged the participants to provide feedback on the app's performance and design for improvements in future updates. We conducted the study online, remotely, and without any researcher interference. The study's procedure follows.

After getting participants' online consent, the study procedure began by showing participants a brochure on the value of early app testing from the perspective of usability, design, and security to help disguise the true purpose of the study. Then, we prompted the participant to complete an online questionnaire to capture their demographic data. Afterward, we showed them the name of the app to download from their app store (i.e., Google Play Store or Apple Store). After installation, we instructed them to create an account, complete the app setup, and return to the online questionnaire. Security decisions were recorded at this time. Once participants installed the app and set up their accounts, they returned to the online questionnaire and answered the knowledge quizzes (security and design). Over the next three days, we sent participants messages to check and review different app offerings. Finally, on the third day, they received a follow-up questionnaire that measured the control variables. Finally, we revealed the actual purpose of the study with a debrief and informed them that setting selections did not initiate any additional data collection by the app.

4.3. Item development

We used a combination of established and newly developed scales to operationalize the constructs. For this study, we developed measures for objective security knowledge and the user's decision security level.

4.3.1. Capturing objective security knowledge

In this study, we define two main areas of objective security knowledge: security threats and defense mechanisms. Humans and technology (two main components in information security) can cause and implement both. Security threats can arise from other individuals (i.e., social engineering attacks) or malicious software (i.e., an IT artifact).

Table 1
Decision points breakdown: total, high-level default, and low-level default.

Setting		Description	Secure Decision (Point)	Default Option: High-Level Security Group	Point	Default Option: Low-Level Security Group	Point
Calendar	P (C[1])	Allow app to access your calendar	Off (1)	On	0	On	0
Location	P (C)	Allow app to access your location	Off (1)	Off	1	On	0
Camera	P (C)	Allow app to access your camera	Off (1)	On	0	On	0
Contacts	P (C)	Allow app to access your contacts	Off (1)	Off	1	On	0
Microphone	P (C)	Allow app to access your microphone	Off (1)	On	0	On	0
Storage	P (C)	Allow app to access your storage	Off (1)	Off	1	On	0
Phone	P (C)	Allow app to access your phone calls	Off (1)	On	0	On	0
SMS	P (C)	Allow app to access your text messages	Off (1)	Off	1	On	0
Update Software	S (AI)	Automatically update app software	On (1)	On	1	Off	0
Update Plugins	S (AI)	Automatically update app plugins	On (1)	Off	0	Off	0
Download	S (AI)	Allow downloads from unknown sources	Off (1)	On	0	On	0
Login Alert	S (AI)	Alert when logging in from a new device	On (1)	Off	0	Off	0
Two-Factor Authentication	S (AI)	Require two-factor authentication every time logging in from a new device	On (1)	On	1	Off	0
Pop-ups and Redirects	S (AI)	Allow pop-ups and redirects in the news and social network sections	Off (1)	Off	1	On	0
Ads	S (AI)	Allow adds from third parties to be shown within the app	Off (1)	On	0	On	0
Cookies	S (AI)	Allow the app to save cookies from your search history	Off (1)	Off	1	On	0
Security Level Points (Total):16				High-Level Security Default Points: **8**		Low-Level Security Default Points: **0**	

[1] P (C): Privacy (Confidentiality), S (AI): Security (Availability &/or Integrity).

Similarly, humans or technology can implement defense mechanisms. Some defense mechanisms are human-oriented (e.g., selecting a strong password, following best practices in public Wi-Fi), whereas others are technology-oriented (e.g., VPNs, firewalls). To use this definition as a basis for accurately measuring the objective security knowledge of personal users, we developed a new scale for this study to fit our general audience in the context of personal security. We followed a recent framework that Boateng et al. [97] proposed for developing and validating scales for behavioral sciences, integrating this procedure with several steps that previous IS literature [52,89,98] proposed and used. The final scale was a 20-item multiple-choice quiz (see Appendixes 1 and 2).

To measure subjective security knowledge, we adopted a standard scale from Alba and Hutchinson [6]. We measured subjective security knowledge by asking the participants to estimate how many questions they thought they answered correctly after answering the objective security knowledge quiz. To operationalize high- vs. low-level security default settings, we created two groups of default settings. For the first group, labeled as the high-level security default settings, 50% of the options were selected securely, leading to a security level of eight points. This design created an opportunity for users to improve their security posture. Operationalizing the default settings' security level allowed us to assess its relationship with the user's decision of security level, in a controlled and meaningful way, and emulate the existing approaches in setting up default settings, discussed earlier. *These options were randomly selected but were the same for all individuals in the group.* For the second group, labeled as low-level security default settings, none of the options was selected in a secure state, leading to a security level of 0 points. Table 1 illustrates how participants in each group saw the settings when they set up an account.

4.3.2. Control variables

Based on our literature review, we used several control variables for dependent constructs in the model. For subjective security knowledge, we controlled self-efficacy, age, IT experience, IT education, and gender [6, 11,52]. Many prior security studies have used behavioral intentions in various contexts as the main constructs. However, to be conservative, we controlled for many of the factors often controlled for intention constructs for our dependent construct (an actual decision) to avoid the influence of confounding factors. Thus, for the user's decision security level, in addition to the previously described variables, we used other control variables (see Appendix 3), including phone usage experience (in years), daily phone usage, perceived threat severity, perceived threat susceptibility, impulsivity, social norms, and descriptive norms [1,52,85].

4.4. Sample

We recruited participants through Prolific.co, an online labor market for research, which allowed us to diversify the sample demographics (e.g., age, gender). A total of 100 subjects participated in the study. Five participants did not return or failed to complete the post-study questionnaire or failed to prove that they installed and used the app. We removed them before the analysis.

The final pool of 95 participants included 41 men (43%) and 54 women (57%). Forty-five participants downloaded and installed the app on an IOS device from Apple Store and 50 subjects downloaded and installed the app from Google Play Store. To further assess the quality of data, we used premium features in the Prolific platform and a series of manual checks. First, we used features in the online platform that verified worker-country locations and features that blocked duplicate IP addresses as well as any suspicious geocode locations. The manual check included looking for any speeders (i.e., participants who answered the questions, in either the first questionnaire or post-study questionnaire, in less than 40% of the median time of all individuals). We also embedded two attention checks in the questions. The first was a question that asked participants to select a particular answer. The other attention check was a duplicate question that appeared on different pages of the questionnaire, for which we checked whether the answers were similar or different. We also looked for any pattern and duplicate responses from the same latitude and longitude locations. We identified no problematic cases. Furthermore, to check that the users' decisions in the app

were the result of deliberate decision-making, we looked at the time spent in the app and their engagement in the settings section. To operationalize the latter, we specifically looked at how many options users changed during their decision-making. As Appendix 4 shows, the majority of participants actively engaged in the app and made decisions. For the 20% who accepted the default settings with no changes, we looked again for any sign of speeding in tasks (including the questionnaires) and found no red flags for those participants.

4.5. Data analysis

4.5.1. Descriptive analysis

We began our analysis by screening the 95 responses. There was no missing data for variables of interest in the dataset. We observed fairly normal distributions for the indicators of latent factors and all other variables (e.g., age, experience) in terms of skewness and kurtosis. The kurtosis values ranged from benign to 3. Although this does violate strict rules of normality, it is within more relaxed rules that Sposito et al. [99] suggested, recommending 3.3 as the upper threshold for normality. Furthermore, participants randomly received either the low-level (45 participants) or the high-level (50 participants) security default settings at the beginning of the study. Table 2 and Table 3 show the descriptive statistics for the continuous constructs the study used. We also calculated the bivariate correlation, as Table 4 shows (see Appendix 5 for the full table).

4.5.2. Measurement model

Because the study's main construct was measured objectively, we did not foresee any issue with common method bias. However, we followed the measurement model procedure for the latent control variables. To examine the construct validity (divergent and convergent) of the latent control constructs in the study, we conducted an exploratory factor analysis (EFA). EFA is a well-established and common method that determines which items closely correlate to each other and likely represent the same underlying constructs [100]. We used several statistical tests and graphical representations to assess the EFA results. After removing one item that was correlating with multiple underlying constructs, the validity and reliability of the remaining model were supported. Following the EFA, we conducted a confirmatory factor analysis (CFA) to confirm the latent control constructs' structure. CFA follows EFA to finalize the items the structural model used [101]. Ultimately, one item with loading below 0.60 was removed, and we retained the rest (see Appendix 6 for a summary of the results). Next, we assessed the data for the presence of multicollinearity by calculating the Variance Inflation Factor (VIF) for each of the independent variables. One of the more conservative sources on thresholds [102] considers VIF below 3 not problematic. Most VIF values were below 2, with the highest (i.e., age) being slightly above 2 (Appendix 7 shows the full analysis). Accordingly, we found no multicollinearity issue regarding the independent variables [102]. Last, we calculated Cook's D to see if there were any influential outliers that warranted further investigation. Using 4/n, where n = the number of subjects in the data [103], we found no issue with influential outliers.

To examine the model, we proceeded with structural equation modeling (SEM) using AMOS [104] (Appendix 8). The structural model had two stages (i.e., with no control variables and including control variables). The analysis first examined the model fit indices. Once passed according to existing thresholds [105–107], we examined the squared multiple correlations (analogous to R^2 in Ordinary Least Squares regression) to ensure that the variance the study's model explained was sufficient to meaningfully contribute to the field. Finally, we examined the estimates pertinent to the hypotheses.

4.5.3. Structural model results

The complete model (with control variables included) explains 35% of the subjective security knowledge and 34% of the security level of the user's decision variance (Table 5). Objective security knowledge had an insignificant impact on the user's decision security level (β=0.17, $p = 0.09$), despite having a significant positive bivariate correlation with the user's decision security level ($r = 0.28$); thus, it did **not support H1**. Default settings' security level had a positive influence on the user's decision security level, in which participants with a high-level security default option ultimately decided to select overall higher-level security settings (β=0.32, $p < 0.01$), **supporting H2**. Objective security knowledge positively influenced subjective security knowledge (β=0.43, $p < 0.01$), **supporting H3**. Subjective security knowledge positively influenced the user's decision security level (β=0.29, $p < 0.01$), **supporting H4**. Results are displayed in Fig. 3.

4.5.4. Post Hoc analysis

In addition to the direct relationship among the three primary independent constructs of this study (i.e., objective security knowledge, subjective security knowledge, and default security settings) with the dependent construct (i.e., user's decision security level), an assessment of potential moderating and mediating relationships can provide additional insight, not only from a theoretical perspective but also from a practical viewpoint. Two post hoc analyses are of interest in this study.

First is the mediating effect of subjective security knowledge between objective security knowledge and the user's security decision. As suggested in prior literature [11,13,23] and shown in our current study, objective security knowledge positively impacts subjective security knowledge. Furthermore, subjective security knowledge, as a form of self-referent thought, can be integral in decision-making [24,25]. Accordingly, examining whether subjective security knowledge mediates objective security knowledge is important from a theoretical perspective because it can provide evidence of such an effect in the context of cybersecurity decision-making. From a practical standpoint, such relationships can provide a new educational angle that can assist organizations in addressing the knowledge–doing gap [18].

For the mediation analysis, we used Hayes's bootstrap 90% bias-corrected approach [108], using 2000 samples. The indirect effect of objective security knowledge and subjective security knowledge on the user's decision security level was significant (β=0.22, $p < 0.05$). Interestingly, subjective security knowledge fully mediated the influence of objective security knowledge on the user's decision security level; we saw no significant path between objective security knowledge and the user's decision security level when subjective knowledge was included in the model.

The second post hoc analysis concerns the potential moderating effect of objective and subjective security knowledge on the relationship between default security settings and the user's decision security level. Default settings can be used as an anchor [26], creating a default pull [92]. Recall that this occurs in a two-step process of comparative assessment, where users judge whether they prefer alternatives over the default settings, and absolute judgment, where they make the final decision. Knowledge can play an essential role in the influence of defaults; Epley [76] points out that during comparative assessment, decision-makers will retrieve their context-related knowledge to assess the anchor. Thus, objective and subjective security knowledge can potentially moderate how individuals use default settings in their final decisions. As shown in our study, default settings' security level had a significant positive relationship with a user's decision security level, posing either benefits or risks (i.e., more/less secure defaults lead to more/less secure decisions by users). However, the question is: Can knowledge moderate this relationship? Theoretically, understanding debiasing tools is equally important, if not more, than discovering biases [109–111]. In cybersecurity, this potential moderation is important because if such moderation exists, knowledge can be used as a debiasing mechanism, leading people to rely on a more objective decision rather than one heavily anchored by defaults. Discovering debiasing tools in the age in which human errors are still the primary cause of major breaches [20–22] has significant practical implications for organizations as well.

Table 2
Descriptive statistics for main continuous constructs.

Construct	Range	Min	Max	Mean	StdDev	Skewness	Kurtosis
Objective Security Knowledge	[0, 20]	4	19	13.18	2.69	−0.49	0.42
Subjective Security Knowledge	[0, 20]	4	20	11.48	3.22	0.18	−0.26
User's Decision Security Level	[0, 16]	0	16	8.54	4.64	−0.71	−0.45

Table 3
Descriptive statistics for user's decision security level by default groups.

Default Group	Average	Min	Max	StdDev
Low-Level Security Default (0 points)	7.07	0.00	15.00	5.87
High-Level Security Default (8 points)	9.86	5.00	16.00	2.57
Combined Total	8.54	0.00	16.00	4.64

Note: None (eight) of the settings was (were) set to secure option in Low-Level (High-Level) Security Default.

Table 4
Bivariate correlations for main constructs.

		1	2	3	4
1	User's Decision Security Level				
2	Objective Security Knowledge	0.28**			
3	Subjective Security Knowledge	0.30**	0.50**		
4	Default Settings' Security Level	0.30**	0.09	−0.05	

Note. $N = 95$, $*p < 0.05$; $**p < 0.01$.

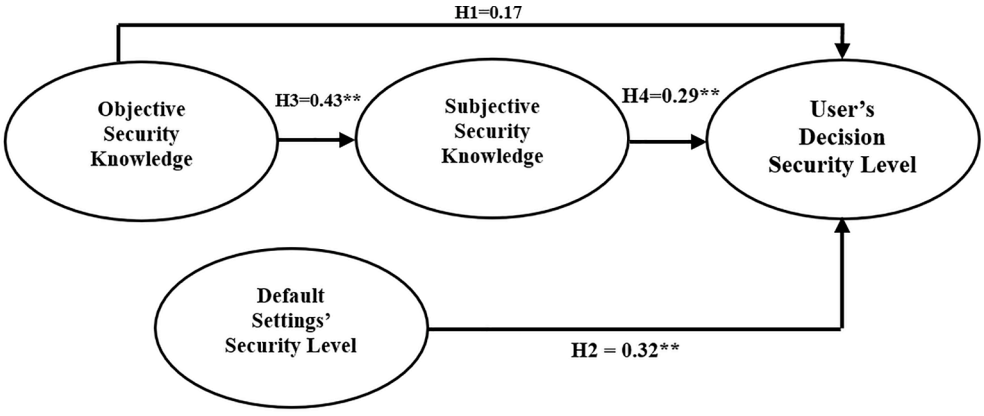
Table 5
Squared multiple correlation.

Construct	Variance Explained No Control	Variance Explained with Control
Subjective Security Knowledge	0.25	0.35
User's Decision Security Level	0.22	0.34

Accordingly, we conducted two moderation analyses on subjective and objective security knowledge and their interaction with the default security setting and user's decision security level relationship. We found that subjective security knowledge attenuated the influence of default settings' security level on the user's decision security level (β=−0.22., $p<0.05$). However, objective security knowledge had no such moderating effect (β=−0.01., $p = 0.88$). This finding further highlighted the key role of subjective security knowledge from both a practical and theoretical perspective.

5. Discussion

Concerning potential influences on users' decision security level, we hypothesized three main effects, two of which were supported in this study. Both increases in subjective security knowledge and default settings' security level led to an increase in the user's decision security level. We observed that higher-level objective security knowledge led to higher-level subjective security knowledge. Further, enhancements in the default settings (high-level security) led to an increase in the user's decision security level. However, the data did not support H1, in which we predicted that an increase in objective security knowledge would lead to an increase in the security level that users selected. We attributed this finding to the mediation effect of subjective security knowledge. Subjective security knowledge (what users think they know) transmits the effect of objective security knowledge (what users actually know). Our results correspond with findings in the finance literature, where subjective knowledge has a positive association with financial well-being [30], and align with Bandura's statement on the role of self-referential thought [22]. Specifically, having adequate knowledge is not enough to lead to proper action. One must also possess higher-level subjective knowledge.



Notes:

- *$* p<.05$, $** p<.01$, MSC= Multiple Squared Correlation ($\sim R^2$)*
- *Model Fit Indices: $\chi 2/DOF= 1.18$, CFI= 0.98, RMSEA= 0.04, PCLOSE= 0.47, Standardized RMR= .02*
- Control variables on subjective security knowledge: *self-efficacy, age, IT experience, IT education, gender*
- Control variables on the user's decision security level: *phone usage experience (in years), daily phone usage, perceived threat severity, perceived threat susceptibility, impulsivity, social norms, descriptive norms, self-efficacy, self-efficacy, age, IT experience, IT education, and gender*

Fig. 3. SEM Results.

Furthermore, in addition to mediating the influence of objective knowledge on users' decision security level, we observed that as subjective security knowledge increases, the influence of default settings on users' decisions decreases. Table 6 breaks down the users' decision security levels in a 2 × 2 (default settings' security level: high-level security/low-level security × high subjective security knowledge/low subjective security knowledge[1]) group structure. The impact of defaults is greater for people with lower-level subjective security knowledge than average (participants with high-level security defaults scored more points than those with low-level security defaults). However, for people with higher-level subjective security knowledge than average, the influence of the default is less (high-level security default scored two points higher than those with low-level security default).

Finally, the findings are also partially in line with the proposition discussed in relation to the Dunning-Kruger effect [112]. The Dunning-Kruger effect was among the frameworks developed after the inception of bounded rationality [112,113]. In their original study, the authors relied on knowledge (similar to objective knowledge) and metacognition (analogous to subjective knowledge), also called self-monitoring skills [114]. According to the Dunning-Kruger effect, incompetent individuals face a dual burden. Those who lack objective knowledge not only make worse decisions but also lack the metacognition to be aware. Thus, they overestimate their own performance and see themselves as above average. Those individuals who are competent suffer a somewhat reverse pattern; they perform well but underestimate their performance compared with their peers [112]. The Dunning-Kruger effect is not fully applicable to this study because that effect examines the assessment of both self versus self as well as that of self versus others (i.e., the above-average effect). Additionally, the effect suggests that highly competent individuals underestimate their performance compared with others and not compared with their own actual performance. Finally, the effect focuses on trivial questions and tasks that may not have personal relevance for individuals (unlike a security context) [113]. However, there is one area of applicability: the effect discusses that, as people become more knowledgeable, they also gain the metacognition to understand the limits of their knowledge and performance. To assess whether our study provides evidence on this proposition, we categorized participants into four groups of high- and low-level subjective and objective security knowledge, based on their mean score. As Fig. 4 shows, the results highlight that most individuals in the high-level objective knowledge group (32 of 46) also possessed high-level subjective security knowledge. A proposition found in both the Dunning-Kruger effect and bounded rationality; the more knowledgeable one is, the better one understands the scope and limits of their limitations [94,112]. Interestingly, there is minimal difference among the three other groups. In other words, our data suggest that individuals with high objective knowledge will perform the same as those with low objective knowledge, absence of high subjective security knowledge. This can potentially explain the high error rates [22] and the know–-doing gap [18] in cybersecurity decision-making. Hence, findings suggest that objective security knowledge (often considered the only integral form of knowledge used in public and organizational training) alone will not lead to the most secure decisions.

Table 6
Moderating role of subjective security knowledge in the relationship between default settings' security level and the user's decision security level.

	Low Subjective Security Knowledge	High Subjective Security Knowledge
Low-Level Security Default (0 Points)	5.6	8.6
High-Level Security Default (8 points)	9.2	10.7

[1] Mean subjective security knowledge (M = 11.48) was the criterion for separating users into high or low groups.

5.1. Theoretical implications

This study offered several theoretical implications. Most notably, it underscored the vital role of subjective security knowledge. First, the results showed that subjective security knowledge helps with the utilization of objective security knowledge. Thus, even if people are objectively knowledgeable in information security, they will not act on that knowledge without high-level subjective knowledge. Consequently, subjective security knowledge acts as a conduit between objective security knowledge and security decisions, propelling users to apply their knowledge when deciding whether to act.

"Knowledge, transformational operations, and component skills are necessary but insufficient for accomplished performances. Indeed, people often do not behave optimally, even though they know full well what to do. This is because self-referent thought also mediates the relationship between knowledge and action." [16, p. 122]

We see this as an important implication because subjective security knowledge can enhance users' performance, a distinct approach compared with the common approach of presenting users with nudges aimed at increasing their knowledge [3]. Feedback can manipulate subjective knowledge by showing users their self-assessment and their actual performance on a quiz [110].

Second, subjective security knowledge can act as a debiasing mechanism to counter status quo bias. Epley [91] points out that, during comparative assessment (where users judge whether they prefer alternatives over the default settings), decision-makers will retrieve their context-related knowledge to assess the anchor. We argue that this is where subjective knowledge moderates the influence of the default settings' security level on a user's chosen decision security level. Specifically, higher-level subjective security knowledge means that the user believes their security knowledge level is higher. Because biases (i.e., errors in judgment) can lead to adverse outcomes for decision-makers, researchers aimed to identify techniques that combat such biases [109,110]. In this study, subjective security knowledge dampened the positive relationship between default settings security and the user's decision security level. This finding contributes not only to the information security literature but also to the broader IS literature. With default options present in many IT domains (e.g., investment, IT use, adoption), status quo bias can cause individuals or firms to stay with their current choice rather than objectively considering other alternatives. However, subjective knowledge can potentially reduce the influence of default options and essentially "debias" the decision-makers. Future investigations can shed light on this potential impact in the broader IS literature.

Additionally, we observed that participants anchor their final decisions on the default settings, thus facing more or less secure final decisions depending on the default settings' level of security. However, with higher degrees of subjective security knowledge, users will be less likely to follow the default settings and more likely to make their own decisions. Combining the will to make one's security decisions with a higher degree of objective security knowledge, users can increase the security level of their decisions while avoiding status quo bias.

Furthermore, as predicted, we observed a positive association between default settings' security level and objective security knowledge with users' decision security level. However, this more nuanced relationship has two implications. First, the role of default settings in increasing users' online security should not be overlooked; and second, the emphasis on user education should go beyond objective security knowledge to ensure more secure decisions. Between the two constructs, the default settings' security level was associated more strongly than objective security knowledge with the security level of users' decisions. This finding showed the strong effect of the "default pull" in the context

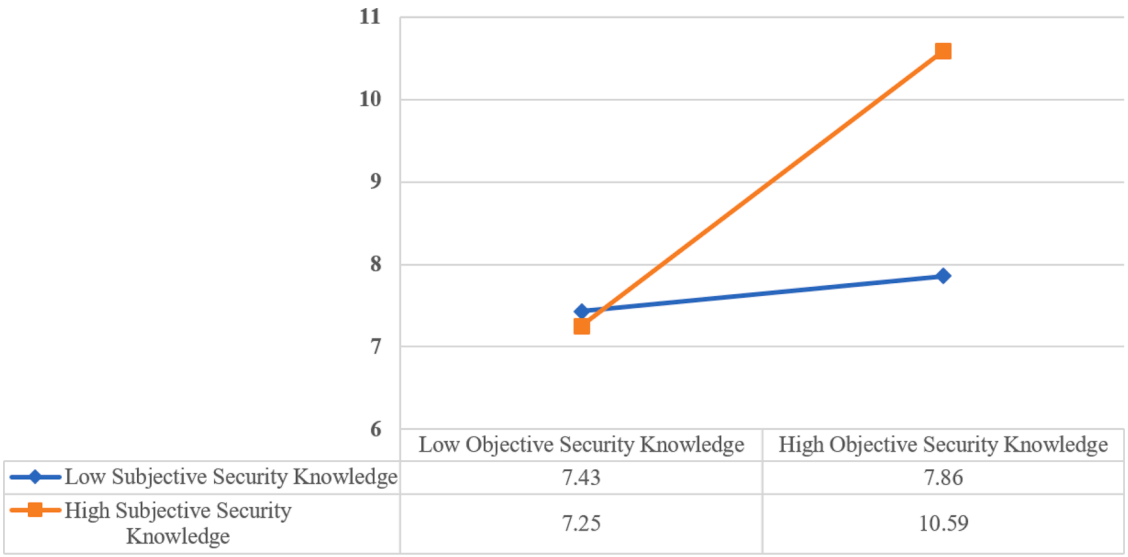


Fig. 4. Average Decision Score in a 2 (High vs. Low) × 2 (Objective vs. Subjective) Model.

of information security. Additionally, despite a positive correlation between objective security knowledge and the security level of users' decisions, we observed that objective security knowledge did not significantly predict the dependent construct if considered in conjunction with subjective security knowledge and other control constructs. This result showed that the security knowledge one has, although integral, is insufficient for taking action if subjective knowledge is absent. Thus, platforms and apps should prompt users to think about their performance in the security option selection process.

5.2. Practical implications

According to industry reports, companies and institutions, such as universities, e-retailers, and social media platforms, offer services to individuals who constantly face security breaches. E-bay, LinkedIn, Yahoo, Facebook, and Target have all experienced massive security breaches in recent years [115], and universities have also faced a rise in security threats [116]. Organizations follow in the same footsteps by offering educational programs regarding security to their employees. Various security threats each require a specific countermeasure strategy. For instance, threats can occur because of weak information security infrastructure, lackluster oversight or the actions of a malicious employee, and poor user security decisions among users. In this study, we focused on the security decisions of personal users, which can either exacerbate or alleviate existing security threats. For example, weak passwords were one of the factors that worsened the 2016 LinkedIn password security breach, which led to the sale of 117 million records on the dark web [117]. Pertinent to combating security threats related to poor security decision-making, we argue that our findings have several practical implications for designers, educators, and organizations that provide services.

The first practical implication is that the designer of security education materials should expand their focus beyond just objective security knowledge to other behavioral and environmental factors (as Simon discusses in relation to the theory of bounded rationality). In recent years, various governments have coordinated efforts to increase public knowledge of information security. For example, the governments of Canada and the United States offer educational websites and brochures on best security practice guidelines, focusing solely on enhancing objective security knowledge. Based on this study, two other factors must be considered for integration into these programs. First, we believe that raising users' subjective security knowledge—so long as it is based on their objective security knowledge—should be a priority in feedback and online learning tools. Currently, online security programs assess users' objective security knowledge. In a simple learning format, security training provides several educational pages, quizzes users on those materials, and provides a test score.

We believe creating mechanisms to provide feedback regarding users' subjective security knowledge has value. We suggest that to do so, one must first ask about users' perception of their performance before showing the actual results of the assessment. Subsequently, having captured their subjective security knowledge, the system displays the final score on the assessment (i.e., objective security knowledge) and users' self-assessment. Displaying these two numbers in juxtaposition allows users to compare their self-assessment to their actual performance. This form of feedback allows users to adjust their knowledge-specific self-assessment accordingly, thus enhancing their subjective security knowledge alongside their objective security knowledge [118].

Second, we show that default settings play a crucial role in enhancing users' security. Default settings are one of the best tools for designers and organizations to push individual users toward more secure decisions. The tendency to anchor security decisions using the default settings is a great opportunity for designers to help users enhance online security. However, many approach default settings with a "user preference first" mentality and do not offer secure options as a default. Many popular websites, such as Facebook, Instagram, or even Google, do not present by default all their settings for high-level security. For example, when creating a new account at the time of this study, these websites mostly had the options turned off, leaving it up to users to select more secure options in their settings; however, many users do not change their settings. Anecdotal evidence also exists for user acceptance of default settings on registration. A report from 2013 shows that nearly 13 million Facebook users never changed their privacy settings [119]. Regardless of what causes this status quo bias, the phenomenon is important in users' security decision-making. As Appendix 4 shows, the respective proportions of individuals in the high- and low-level security groups who did not change their default settings were identical (i.e., approximately 22%), hinting that some users could not distinguish between high- or low-level security default options or simply did not care to change them.

Consequently, default settings can act as a double-edged sword. From one perspective, they can lead to decisions with a lower security level and be a great opportunity for hackers or malicious developers to steal customers' data. For example, blindly giving permission to a smartphone app can cause data loss and an invasion of privacy. In web accounts, lack of proper setup for security settings can cause loss of access to the account in case of unauthorised intrusion. From another

perspective, this is an opportunity for designers and developers to assist novice users with their security decisions. For instance, by turning on "login alert from a new device" by default, it is more likely that a user will keep this option on, enhancing their personal information security. Although our study showed that subjective security knowledge could combat status quo bias, the best practical implication is to have a dual focus: increase users' subjective security knowledge proportionate to their actual knowledge and present the most secure settings by default.

5.3. Future directions

The findings of the current study open several avenues for future research. First, the role of subjective security knowledge can be assessed in group security decision-making contexts in which herd behavior may be present [45]. Similar to status quo bias, herding leads users to make decisions based on an initial anchor (default settings vs. others' decisions). Does a higher level of subjective security knowledge reduce herding behavior as it did status quo bias? Another avenue is to examine security decision-making in a context where security conflicts with usability. Although our context involved no tangible tradeoff between app security and usability, there are situations in which secure choices will significantly reduce technology usability. The next step for this research route is to further examine those contexts.

Finally, future studies could investigate how a three-state default structure can work. In this default design, a null state can be added to "on" and "off" states. The motivation behind this design is that an option will be neither on nor off in this null state. Instead, the user must decide to either turn it on or off. In other words, what happens if we remove the current anchor (on vs. off) in the default settings that all users see? What happens if the default pushes users to make a decision without any predisposition to an on or off state? Can system messages or other techniques persuade users to make secure decisions in this case? If such a design becomes commonplace, can it prevent malicious actors from misusing default settings?

5.4. Limitations

It can be argued that two of the temporal choices in the operationalization of the study are conceptually out of order: showing the knowledge quiz after the decision and measuring subjective security knowledge after the quiz. First, the choice to show the quiz after the decision was to avoid priming the participants. If we were to ask them to install the app after taking the quiz, participants would have discovered the purpose of the study and may not have behaved in an unbiased manner. Second, the choice to assess subjective knowledge immediately after the knowledge quiz stemmed from validated procedures used in prior studies [6,23]. Although we weighed the cost and benefits of the order of the actions in the study and ultimately found this to be the best approach and one that is backed by prior studies, it still can be considered as a limitation. Additionally, we do not comment on the impact of individual settings (e.g., 2FA) on security decisions. Rather, our focus is on aggregate decisions. This led to several procedural decisions for the study, such as using a fixed form of default settings for all participants rather than a randomized one for each participant. Although this decision was meant to avoid confounding factors, it is nonetheless a limitation on which future research could expand. Additionally, although we strived to improve our methodology to achieve both relevance and rigor by improving the ecological validity of the study, our context is focused on campus life, warranting further research into other contexts in the future. However, we believe that our results are somewhat conservative. We strived to conduct the study in a context with relevance and importance by designing an app from scratch and asking participants to use it on their personal devices. However, limitations regarding relevancy exist, and in other, more sensitive contexts, such as health care or finance, we would expect stronger results and, especially, a greater role for subjective security knowledge in action.

6. Conclusion

In today's interconnected world that has experienced a global pandemic, users make many security-related decisions daily and are vulnerable to numerous security threats. Objective security knowledge and secure default settings have been two essential tools that help users make secure decisions. However, human errors resulting from a lack of utilization of objective security knowledge and an overreliance on low-level security default settings pose issues. In this study, we investigated the role of subjective security knowledge (i.e., what a person thinks of their security knowledge) alongside default settings and objective security knowledge in information security decision-making. Based on the theory of bounded rationality, the findings showed that subjective security knowledge not only mediates the impact of objective security knowledge on users' decision security level but also reduces the tendency to blindly accept default security settings.

Funding

This study was funded by The Social Sciences and Humanities Research Council (SSHRC) by government of Canada and Scotiabank.

CRediT authorship contribution statement

Amir Fard Bahreini: Conceptualization, Methodology, Writing – original draft, Investigation, Project administration, Formal analysis. **Hasan Cavusoglu:** Conceptualization, Methodology, Writing – review & editing, Funding acquisition, Supervision, Software, Resources. **Ronald T. Cenfetelli:** Conceptualization, Methodology, Writing – review & editing, Funding acquisition, Supervision, Validation.

Declaration of competing interest

There is no conflict of interest (financial/personal) between the authors and this study.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.im.2023.103860.

References

[1] C.L. Anderson, R. Agarwal, Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions, MIS Q. (2010) 613–643.
[2] A. Acquisti, L. Brandimarte, G. Loewenstein, Privacy and human behavior in the age of information, Science 347 (6221) (2015) 509–514.
[3] A. Acquisti, et al., Nudges for privacy and security: understanding and assisting users' choices online, ACM Comput. Surveys (CSUR) 50 (3) (2017) 1–41.
[4] Verizon, Data Breach Investigations Report, 2022 [Online]. Accessed March 1, 2022. Available, https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf.
[5] IBM, Cost of a Data Breach Report 2022, 2022 [Online]. Accessed June 1, 2022, Available, https://www.ibm.com/downloads/cas/3R8N1DZJ.
[6] J.W. Alba, J.W. Hutchinson, Knowledge calibration: what consumers know and what they think they know, J. Consumer Res. 27 (2) (2000) 123–156.
[7] P. Puhakainen, M. Siponen, Improving employees' compliance through information systems security training: an action research study, MIS Q. (2010) 757–778.
[8] M. Silic, P.B. Lowry, Using design-science based gamification to improve organizational security training and compliance, J. Manag. Inf. Syst. 37 (1) (2020) 129–161.
[9] Government of Canada, GetCyberSafe, 2022. Accessed March 15, 2022, https://www.getcybersafe.gc.ca/en/resources.
[10] National Security Agency, Best Practices for Keeping Your Home Network Secure, 2018. Accessed March 15, 2022, https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/csi-best-practices-for-keeping-home-network-secure.pdf.
[11] M. Brucks, The effects of product class knowledge on information search behavior, J. Consumer Res. 12 (1) (1985) 1–16.
[12] C.W. Park, D.L. Mothersbaugh, L. Feick, Consumer knowledge assessment, J. Consumer Res. 21 (1) (1994) 71–82.

[13] P.S. Raju, S.C. Lonial, W.G. Mangold, Differential effects of subjective knowledge, objective knowledge, and usage experience on decision making: an exploratory investigation, J. Consumer Psychol. 4 (2) (1995) 153–180.
[14] C. Moorman, K. Diehl, D. Brinberg, B. Kidwell, Subjective knowledge, search locations, and consumer choice, J. Consumer Res. 31 (3) (2004) 673–680.
[15] A. Lusardi, O.S. Mitchell, Baby boomer retirement security: the roles of planning, financial literacy, and housing wealth, J. Monet. Econ. 54 (1) (2007) 205–224.
[16] S.M. Furnell, P. Bryant, A.D. Phippen, Assessing the security perceptions of personal Internet users, Comput. Security 26 (5) (2007) 410–417.
[17] LastPass, Psychology of Passwords: How to Password Hygiene Reduces Your Password Security Risk, 2020. Accessed November 21, 2021, https://www.lastpass.com/resources/psychology-of-passwords-2020.
[18] M. Workman, W.H. Bommer, D. Straub, Security lapses and the omission of information security measures: a threat control model and empirical test, Comput. Human Behav. 24 (6) (2008) 2799–2816.
[19] V.J. Calluzzo, C.J. Cante, Ethics in information technology and software use, J. Bus. Ethics 51 (2004) 301–312.
[20] M. Sher-Jan, Data Indicates Human Error Prevailing Cause of breaches, Incidents, 2018. Accessed November 22, 2021, https://iapp.org/news/a/data-indicates-human-error-prevailing-cause-of-breaches-incidents/.
[21] PwC, U.K. Information Security Breaches Survey, 2013 [Online]. Accessed September 22, 2020. Available, https://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf.
[22] Verizon, Data Breach Investigation Report, 2020. Accessed November 2, 2021, https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf.
[23] J.P. Carlson, L.H. Vincent, D.M. Hardesty, W.O. Bearden, Objective and subjective knowledge relationships: a quantitative analysis of consumer research findings, J. Consumer Res. 35 (5) (2009) 864–876.
[24] A. Bandura, Self-Efficacy: The Exercise of Control, Macmillan, 1997.
[25] A. Bandura, Self-efficacy mechanism in human agency, Am. Psychol. 37 (2) (1982) 122.
[26] W. Samuelson, R. Zeckhauser, Status quo bias in decision making, J. Risk Uncertain. 1 (1) (1988) 7–59.
[27] Statista, Number of Apps Available in Leading App Stores As of 3rd Quarter 2022, 2022. Accessed May 31, 2022, https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/.
[28] T. Armeding, Mobile Apps: Still Insecure By Default, 2019. Accessed May 25, 2021, https://www.forbes.com/sites/taylorarmerding/2019/06/27/mobile-apps-still-insecure-by-default/?sh=3832ad783b24.
[29] S. Brown, The Data Privacy Tips Digital Security Experts Wish You Knew, 2022. Accessed May 25, 2022, https://www.cnet.com/tech/services-and-software/the-data-privacy-tips-digital-security-experts-wish-you-knew/.
[30] J. Vijayan, Many Mobile Apps Intentionally Using Insecure Connections For Sending Data, 2021. Accessed May 15, 2022, https://www.darkreading.com/mobile/many-mobile-apps-intentionally-using-insecure-connections-for-sending-data/d/d-id/1341276.
[31] J. Khalili, Tens of Thousands of Malicious Android Apps Flooding User Devices, 2020. Accessed April 25, 2022, https://www.techradar.com/news/tens-of-thousands-of-malicious-android-apps-flooding-google-play-store.
[32] B. Toulas, Android Malware Apps With 2 Million Installs Found On Google Play, 2022. Accessed December 10, 2022, https://www.bleepingcomputer.com/news/security/android-malware-apps-with-2-million-installs-found-on-google-play/.
[33] H.A. Simon, Bounded rationality in social science: today and tomorrow, Mind & Soc. 1 (1) (2000) 25–39.
[34] H.A. Simon, Theories of bounded rationality, decision and organization, CBR a. R. Radner. Amsterdam, NorthHolland (1972).
[35] H.A. Simon, Theories of bounded rationality, Decision and Organ. (1972) 161–176.
[36] D. Diakoulaki, G. Mavrotas, L. Papayannakis, Determining objective weights in multiple criteria problems: the critic method, Comput. Oper. Res. 22 (7) (1995) 763–770.
[37] A.R. Dennis, R.K. Minas, Security on autopilot: why current security theories hijack our thinking and lead us astray, ACM SIGMIS Database: The DATABASE for Adv. Inf. Syst. 49 (SI) (2018) 15–38.
[38] R.W. Rogers, A protection motivation theory of fear appeals and attitude change, J. Psychol. 91 (1) (1975) 93–114.
[39] H. Liang, Y. Xue, Avoidance of information technology threats: a theoretical perspective, MIS Q. (2009) 71–90.
[40] D. Ariely, S. Jones, Predictably Irrational, HarperCollins New York, 2008.
[41] A. Acquisti, L.K. John, G. Loewenstein, The impact of relative standards on the propensity to disclose, J. Mark. Res. 49 (2) (2012) 160–174.
[42] H. Li, R. Sarathy, J. Zhang, The role of emotions in shaping consumers' privacy beliefs about unfamiliar online vendors, J. Inf. Privacy and Security 4 (3) (2008) 36–62.
[43] J. D'Arcy, P.B. Lowry, Cognitive-affective drivers of employees' daily compliance with information security policies: a multilevel, longitudinal study, Inf. Syst. J. 29 (1) (2019) 43–69.
[44] T. Dinev, A.R. McConnell, H.J. Smith, Research commentary—Informing privacy research through information systems, psychology, and behavioral economics: thinking outside the 'APCO' box, Inf. Syst. Res. 26 (4) (2015) 639–655.
[45] A. Vedadi, M. Warkentin, Can secure behaviors be contagious? A two-stage investigation of the influence of herd behavior on security decisions, J. Assoc. Inf. Syst. 21 (2) (2020) 3.
[46] A. Burns, T.L. Roberts, C. Posey, P.B. Lowry, The adaptive roles of positive and negative emotions in organizational insiders' security-based precaution taking, Inf. Syst. Res. 30 (4) (2019) 1228–1247.
[47] R. Wash, Folk models of home computer security, in: presented at the Proceedings of the Sixth Symposium on Usable Privacy and Security, 2010, pp. 1–16.
[48] J.Y. Tsai, S. Egelman, L. Cranor, A. Acquisti, The effect of online privacy information on purchasing behavior: an experimental study, Inf. Syst. Res. 22 (2) (2011) 254–268.
[49] S. Herbert, Theories of decision-making in economics and behavioral science, Am. Econ. Rev. 49 (1959) 253–283.
[50] B.L. Lipman, Information processing and bounded rationality: a survey, Canadian J. Econ. (1995) 42–67.
[51] D. Kahneman, A perspective on judgment and choice: mapping bounded rationality, Am. Psychol. 58 (9) (2003) 697.
[52] R. Aggarwal, D. Kryscynski, V. Midha, H. Singh, Early to adopt and early to discontinue: the impact of self-perceived and actual IT knowledge on technology use behaviors of end users, Inf. Syst. Res. 26 (1) (2015) 127–144.
[53] W. Newhouse, S. Keith, B. Scribner, G. Witte, National initiative for cybersecurity education (NICE) cybersecurity workforce framework, NIST Special Publication 800 (2017) 181, 2017.
[54] R. Fredrica, Consumer Food Selection and Nutrition Information, 1979.
[55] C.M. Radecki, J. Jaccard, Perceptions of knowledge, actual knowledge, and information search behavior, J. Exp. Soc. Psychol. 31 (2) (1995) 107–138.
[56] P. Babiarz, C.A. Robb, Financial literacy and emergency saving, J. Fam. Econ. Issues 35 (1) (2014) 40–50.
[57] N. Ben-Asher, C. Gonzalez, Effects of cyber security knowledge on attack detection, Comput. Human Behav. 48 (2015) 51–61.
[58] J. Camp, F. Asgharpour, D. Liu, I. Bloomington, Experimental evaluations of expert and non-expert computer users' mental models of security risks, Proceed. WEIS (2007) 1–24, 2007.
[59] A. Yazdanmehr, J. Wang, Employees' information security policy compliance: a norm activation perspective, Decis. Support Syst. 92 (2016) 36–46.
[60] C. Lee, C.C. Lee, S. Kim, Understanding information security stress: focusing on the type of information security compliance activity, Comput. Security 59 (2016) 60–70.
[61] C. Ament, The ubiquitous security expert: overconfidence in information security, in: ICIS 2017 Proceedings, 2017.
[62] P. Ifinedo, Effects of security knowledge, self-control, and countermeasures on cybersecurity behaviors, J. Comput. Inf. Syst. (2022) 1–17.
[63] T.A. Busey, J. Tunnicliff, G.R. Loftus, E.F. Loftus, Accounts of the confidence-accuracy relation in recognition memory, Psychon. Bull. Rev. 7 (1) (2000) 26–48.
[64] J. Wang, Y. Li, H.R. Rao, Overconfidence in phishing email detection, J. Assoc. Inf. Syst. 17 (11) (2016) 1.
[65] P. Cichy, T.O. Salge, R. Kohli, Privacy concerns and data sharing the internet of things: mixed methods evidence from connected cars, MIS Q. 45 (4) (2021).
[66] C.W. Yoo, J. Goo, H.R. Rao, Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness, Mis Q. 44 (2) (2020).
[67] B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, MIS Q. (2010) 523–548.
[68] L. Hadar, S. Sood, C.R. Fox, Subjective knowledge in consumer financial decisions, J. Mark. Res. 50 (3) (2013) 303–316.
[69] I. Ion, M. Langheinrich, P. Kumaraguru, S. Čapkun, Influence of user perception, security needs, and social factors on device pairing method choices, in: presented at the *Proceedings of the Sixth Symposium on Usable Privacy and Security*, 2010, pp. 1–13.
[70] S.T. Sun, E. Pospisil, I. Muslukhov, N. Dindar, K. Hawkey, K. Beznosov, What makes users refuse web single sign-on? An empirical investigation of OpenID, in: presented at the *Proceedings of the seventh symposium on usable privacy and security*, 2011, pp. 1–20.
[71] B. Ur, et al., "' I added'!'at the end to make it secure': observing password creation in the lab, in: presented at the *Eleventh symposium on usable privacy and security (SOUPS 2015)*, 2015, pp. 123–140.
[72] R.E. Crossler, F. Bélanger, Why would I use location-protective settings on my smartphone? Motivating protective behaviors and the existence of the privacy knowledge–belief gap, Inf. Syst. Res. 30 (3) (2019) 995–1006.
[73] R. Bhagavatula, B. Ur, K. Iacovino, S.M. Kywe, L.F. Cranor, M. Savvides, Biometric authentication on iphone and android: usability, perceptions, and influences on adoption, in: Proceedings of 2015 Workshop on Usable Security, 2015.
[74] B. Ur, J. Bees, S.M. Segreti, L. Bauer, N. Christin, L.F. Cranor, Do users' perceptions of password security match reality?, in: Proceedings of the *2016 CHI Conference on Human Factors in Computing Systems*, 2016, pp. 3748–3760.
[75] A. De Luca, A. Hang, E. Von Zezschwitz, H. Hussmann, I feel like I'm taking selfies all day! Towards understanding biometric authentication on smartphones, in: presented at the *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, 2015, pp. 1411–1414.
[76] A. Wagner, N. Mesbah, Too confident to care: investigating overconfidence in privacy decision making, in: Proceedings of the 27th European Conference on Information Systems (ECIS), Stockholm & Uppsala, Sweden, 2019. June 8-14.
[77] P.J. Hsieh, Healthcare professionals' use of health clouds: integrating technology acceptance and status quo bias perspectives, Int. J. Med. Inform. 84 (7) (2015) 512–523.
[78] H.W. Kim, A. Kankanhalli, Investigating user resistance to information systems implementation: a status quo bias perspective, MIS Q. (2009) 567–582.

[79] H. Almuhimedi, et al., Your location has been shared 5,398 times! A field study on mobile app privacy nudging, in: presented at the *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, 2015, pp. 787–796.
[80] A. Acquisti, R. Gross, Imagined communities: awareness, information sharing, and privacy on the Facebook, in: presented at the *International Workshop on Privacy Enhancing Technologies*, Springer, 2006, pp. 36–58.
[81] L. Dogruel, S. Joeckel, J. Vitak, The valuation of privacy premium features for smartphone apps: the influence of defaults and expert recommendations, Comput. Human Behav. 77 (2017) 230–239.
[82] Y.L. Lai, K.L. Hui, Internet opt-in and opt-out: investigating the roles of frames, defaults and privacy concerns, in: presented at the *Proceedings of the 2006 ACM SIGMIS CPR conference on computer personnel research: Forty four years of computer personnel research: achievements, challenges & the future*, 2006, pp. 253–263.
[83] Y. Liu, K.P. Gummadi, B. Krishnamurthy, A. Mislove, Analyzing facebook privacy settings: user expectations vs. reality, in: presented at the *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, 2011, pp. 61–70.
[84] J. Watson, H.R. Lipford, A. Besmer, Mapping user preference to privacy default settings, ACM Trans. Comput.-Human Interaction (TOCHI) 22 (6) (2015) 1–20.
[85] N. Wang, P. Wisniewski, H. Xu, J. Grossklags, Designing the default privacy settings for Facebook applications, in: presented at the *Proceedings of the companion publication of the 17th ACM conference on Computer supported cooperative work & social computing*, 2014, pp. 249–252.
[86] T. Nakamura, S. Kiyomoto, W.B. Tesfay, J. Serna, Personalised privacy by default preferences-experiment and analysis, in: presented at the International Conference on Information Systems Security and Privacy, SCITEPRESS, 2016, pp. 53–62.
[87] S. Löbner, W.B. Tesfay, T. Nakamura, S. Pape, Explainable machine learning for default privacy setting prediction, IEEE Access 9 (2021) 63700–63717.
[88] D.G. Goldstein, E.J. Johnson, A. Herrmann, M. Heitmann, Nudge your customers toward better choices, Harv. Bus. Rev. 86 (12) (2008) 99–105.
[89] G. Bassellier, I. Benbasat, B.H. Reich, The influence of business managers' IT competence on championing IT, Inf. Syst. Res. 14 (4) (2003) 317–336.
[90] A. Tversky, D. Kahneman, Judgment under Uncertainty: heuristics and Biases: biases in judgments reveal some heuristics of thinking under uncertainty, Science 185 (4157) (1974) 1124–1131.
[91] N. Epley, A tale of tuned decks? Anchoring as accessibility and anchoring as adjustment, The Blackwell Handbook of Judgment and Decision Making (2004) 240–256.
[92] N. Dhingra, Z. Gorn, A. Kener, J. Dana, The default pull: an experimental demonstration of subtle default effects on preferences, Judgm. Decis. Mak. 7 (1) (2012) 69.
[93] G. Suri, G. Sheppes, C. Schwartz, J.J. Gross, Patient inertia and the status quo bias: when an inferior option is preferred, Psychol. Sci. 24 (9) (2013) 1763–1769.
[94] J.E. Russo, P.J. Schoemaker, Managing overconfidence, Sloan Manag. Rev. 33 (2) (1992) 7–17.
[95] M. Van Rooij, A. Lusardi, R. Alessie, Financial literacy and stock market participation, J. Financ. Econ. 101 (2) (2011) 449–472.
[96] A. Fard Bahreini, H. Cavusoglu, R. Cenfetelli, Role of feedback in improving novice users' security performance using construal level and valance framing, in: Proceedings of International Conference on Information Systems (ICIS), 2020.
[97] G.O. Boateng, T.B. Neilands, E.A. Frongillo, H.R. Melgar-Quiñonez, S.L. Young, Best practices for developing and validating scales for health, social, and behavioral research: a primer, Front. Public Health 6 (2018) 149.
[98] S.B. MacKenzie, P.M. Podsakoff, N.P. Podsakoff, Construct measurement and validation procedures in MIS and behavioral research: integrating new and existing techniques, MIS Q. (2011) 293–334.
[99] V. Sposito, M. Hand, B. Skarpness, On the efficiency of using the sample kurtosis in selecting optimal lpestimators, Commun. Statistics-Simulation and Comp. 12 (3) (1983) 265–272.
[100] L.R. Fabrigar, D.T. Wegener, R.C. MacCallum, E.J. Strahan, Evaluating the use of exploratory factor analysis in psychological research, Psychol. Methods 4 (3) (1999) 272.
[101] T.A. Brown, Confirmatory Factor Analysis For Applied Research, Guilford publications, 2015.
[102] R.M. O'brien, A caution regarding rules of thumb for variance inflation factors, Qual. Quant. 41 (5) (2007) 673–690.
[103] R.D. Cook, Detection of influential observation in linear regression, Technometrics 19 (1) (1977) 15–18.
[104] B.M. Byrne, S.M. Stewart, Teacher's corner: the MACS approach to testing for multigroup invariance of a second-order structure: a walk through the process, Structural Equation Model. 13 (2) (2006) 287–321.
[105] J.F. Hair, W.C. Black, B.J. Babin, R.E. Anderson, R.L. Tatham, Pearson new international edition, Multivariate Data Anal. (2014).
[106] R.B. Kline, Principles and Practice of Structural Equation Modeling, Guilford publications, 2015.
[107] D. Hooper, J. Coughlan, M. Mullen, Evaluating model fit: a synthesis of the structural equation modelling literature, in: presented at the 7th European Conference on research methodology for business and management studies, 2008, pp. 195–200.
[108] A.F. Hayes, Beyond Baron and Kenny: statistical mediation analysis in the new millennium, Commun. ‚Monographs 76 (4) (2009) 408–420.
[109] R.P. Larrick, Debiasing," *Blackwell Handbook of Judgment and Decision Making*, 2004, pp. 316–338.
[110] H.R. Arkes, Costs and benefits of judgment errors: implications for debiasing, Psychol. Bull. 110 (3) (1991) 486.
[111] A. Fard Bahreini, R. Cenfetelli, H. Cavusoglu, The role of heuristics in information security decision making, in: Proceedings of the 55th Hawaii International Conference on System Sciences, 2022, pp. 4816–4825.
[112] J. Kruger, D. Dunning, Unskilled and unaware of it: how difficulties in recognizing one's own incompetence lead to inflated self-assessments, J. Personality and Soc. Psychol. 77 (6) (1999) 1121.
[113] D. Dunning, The Dunning–Kruger effect: on being ignorant of one's own ignorance, Adv. Exp. Soc. Psychol. (2011) 247–296.
[114] M. Chi, R. Glaser, E. Rees, R. Steinberg, Advances in the Psychology of Human Intelligence, 1982.
[115] I. Ahmed, The 15 Biggest Data Breaches of the Last 15 Years, 2019. Accessed May 21, 2021, https://www.socialmediatoday.com/news/the-15-biggest-data-breaches-of-the-last-15-years-infographic/560456/.
[116] P. Muncaster, Over Half of Universities Suffered Data Breach in Past Year, 2020. Accessed May 11, 2021, https://www.infosecurity-magazine.com/news/over-half-of-universities-suffered/.
[117] J. Pagliery, Hackers Selling 117 Million LinkedIn passwords, 2016. Accessed May 3, 2021, https://money.cnn.com/2016/05/19/technology/linkedin-hack/.
[118] H.R. Arkes, C. Christensen, C. Lai, C. Blumer, Two methods of reducing overconfidence, Organ. Behav. Hum. Decis. Process. 39 (1) (1987) 133–144.
[119] E. Protalinski, 13 Million US Facebook users Don't Change Privacy Settings, 2012. May 2Access April 22, 2021, https://www.zdnet.com/article/13-million-us-facebook-users-dont-change-privacy-settings/.

Amir Fard Bahreini is an Assistant Professor of Information Technology and Supply Chain Management at the University of Wisconsin-Whitewater. Amir holds a PhD from the University of British Columbia and has obtained his MBA and MSc from the University of Oklahoma. His-research focuses on the role of privacy laws in organizations, risk management, and the contemporary issues in behavioral information security, such as addressing inadvertent human errors, application of cognitive decision models, nudging techniques, and usable security.

Hasan Cavusoglu is an Associate Professor at the Sauder School of Business at the University of British Columbia. He obtained his PhD and MSc from the University of Texas at Dallas. His-research focuses on the managerial and behavioral issues of information security and privacy and employs both empirical and analytical methods. His-work has appeared in premier journals such as Information Systems Research, MIS Quarterly, Management Science, and the Journal of MIS. He served as an Associate Editor for MIS Quarterly.

Ronald T. Cenfetelli is a Professor of Management Information Systems at the University of British Columbia's Sauder School of Business. He conducts research into e-business, online customer service; the strategic uses of information technology; the behavioral and emotional aspects of technology usage; and human-computer interfaces. His-research has been published in MIS Quarterly, Information Systems Research, and the Journal of AIS. He is serving as a senior editor of MIS Quarterly.