Contents lists available at ScienceDirect

Information & Management

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

Effects of the design of mobile security notifications and mobile app usability on users' security perceptions and continued use intention

Dezhi Wu[a], Gregory D. Moody[b], Jun Zhang[c,*], Paul Benjamin Lowry[d]

[a] Department of Integrated Information Technology, University of South Carolina, Columbia, SC, USA
[b] Department of MIS, Lee Business School, University of Nevada, Las Vegas, NV, USA
[c] International Institute of Finance, School of Management, University of Science and Technology of China, Hefei, China
[d] Department of Business Information Technology, Pamplin College of Business, Virginia Tech, Blacksburg, VA, USA

ARTICLE INFO

Keywords:
Mobile device
Mobile security
Human–computer interaction (HCI)
Mobile applications (apps)
Perceived security
Dual-task interference
Mobile security notification (MSN)

ABSTRACT

The explosive global adoption of mobile applications (i.e., apps) has been fraught with security and privacy issues. App users typically have a poor understanding of information security; worse, they routinely ignore security notifications designed to increase security on apps. By considering both mobile app interface usability and mobile security notification (MSN) design, we investigate how security perceptions of apps are formed and how these perceptions influence users' intentions to continue using apps. Accordingly, we designed and conducted a set of controlled survey experiments with 317 participants in different MSN interface scenarios by manipulating the types of MSN interfaces (i.e., high vs. low disruption), the context (hedonic vs. utilitarian scenarios), and the degree of MSN intrusiveness (high vs. low intrusiveness). We found that both app interface usability and the design of MSNs significantly impacted users' perceived security, which, in turn, has a positive influence on users' intention to continue using the app. In addition, we identified an important conundrum: disruptive MSNs—a common approach to delivering MSNs—irritate users and negatively influence their perceptions of app security. Thus, our results directly challenge current practice. If these results hold, current practice should shift away from MSNs that interrupt task performance.

1. Introduction

The adoption of mobile devices continues at an unprecedented rate throughout the world, such that it has become common to own multiple mobile devices. Consequently, the use of mobile applications (i.e., apps) has also grown dramatically. As mobile user experiences are increasingly enriched by various customized apps, apps have inevitably come to involve greater security risks [1,2]. Mobile apps have enabled new and rich functionality, but they also pose security risks to users, because mobile devices contain sensitive and personal data that apps can access, and thus represents a potential security issue. It is crucial to identify mechanisms that can increase users' mobile security awareness and help them make informed decisions about mobile app security management.

It is of great concern that malicious apps (i.e., apps that access or share more data than is required for the functionality or purpose of the app without the express knowledge of the mobile device owner) are frequently detected in official app repositories by both Apple and Google [2–4]. According to Zacks [5], although malware on personal computers has continuously decreased in recent years, the amount of malware on mobile platforms (including both the iOS and Android platforms) continues to increase rapidly, with an compound annual growth rate of about 125 % from 2011 to 2018. In 2019, more than 24,000 malicious mobile apps were detected and blocked every day [6]. Mobile devices, especially those with an Android operating system (OS), are the most vulnerable and most poorly protected computer devices [7].

A key issue in app security is the lack of effective security controls, because traditional controls have not transferred well to the new security and design paradigms of mobile platforms [8]. A related problem is that app users exhibit a serious lack of security awareness [1,9–11]. All app users face issues of data protection and the sharing of data with third parties, but few have access to reliable information about the ramifications of their security choices [8]. According to McDaniel & Enck [12], most users have little knowledge about app security features. Moreover, apps often request nearly unfettered access to mobile device

[*] Corresponding author.
E-mail addresses: dezhiwu@cec.sc.edu (D. Wu), greg.moody@unlv.edu (G.D. Moody), jzhang90@ustc.edu.cn (J. Zhang), Paul.Lowry.PhD@gmail.com (P.B. Lowry).

https://doi.org/10.1016/j.im.2019.103235
Received 13 February 2017; Received in revised form 6 November 2019; Accepted 11 November 2019
Available online 15 November 2019
0378-7206/ © 2019 Elsevier B.V. All rights reserved.

data, which can easily result in malicious access or unnecessary sharing of private data with third parties [2]. Because the majority of users have poor mobile security awareness [11], most users trust apps and their respective branded app stores (e.g., Google Play and Apple's App Store), regarding them as risk free, and grant all apps access to the data stored on their mobile devices. As a result of this perception, users fail to enable their mobile devices' security controls and disregard security warnings during app selection and installation [2,8].

Given that users generally have a poor understanding of app and mobile data security, push notifications from apps have emerged to keep users informed of updates and to improve their security awareness [13]. Mobile security notifications (MSNs), through push technology, have become the main method of alerting users to the presence of incoming calls, messages, emails, and other user activities [14]. Although the purpose of MSNs is to keep mobile devices and users up-to-date through an event-triggered mechanism in which remote servers "push" information or messages to client apps, MSNs have been shown to irritate users because the notifications interrupt their usual flow of activities [15,16]. In many situations, such notifications are unwelcome to app users and ignored or disabled [3,11,17,18]. They not only fail to increase users' security awareness, but also backfire because they irritate users by inducing dual-task interference during app usage.

In our research context, MSN-induced *dual-task interference* refers to the difficulty of paying attention to MSNs while performing other tasks. To carefully process and cope with MSNs, users have to stop their primary tasks on the app. Researchers have explored how notifications can be designed to minimize interruptions of users' primary tasks [14,19–26]. However, in the extant literature, the negative consequences of MSN-induced dual-task interference have not been thoroughly investigated [27], despite the importance of these consequences. In this study, we empirically examine the negative impact of disruptive MSNs on perceived app security and argue that various MSN designs that interrupt users' ongoing primary tasks may not increase users' perceived security and may even decrease it. We propose that when an app user perceives a higher level of security, they will have stronger intentions to continue using the app. In addition to MSN-related design, we propose that app interface usability is another determinant of users' perceived app security. We propose a theoretical model of the joint influence of mobile app interface usability and MSNs on users' perceived security and their intentions to continue using the app.

We test our theoretical model by conducting a 2*2*2 factorial experiment, in which the MSN designs were manipulated based on (1) the levels of MSN disruption and (2) the levels of intrusiveness of MSN in (3) two app usage contexts (utilitarian vs. hedonic context). Our proposed model is largely supported by the data analysis results, which support a comprehensive understanding of how MSNs affect users' perceived security and their intentions to continue using the app.

Our study contributes to the literature by addressing several research gaps. First, this study examines how the design of MSNs and app usability influence users' security perceptions when users do not have sufficient knowledge to accurately assess the app's security level. We posit that users rely heavily on explicit cues to make such assessments. Specifically, we identified two determinants of perceived app security: MSN design and app interface usability. If MSNs are user friendly and designed to avoid dual-task interference and if the app interface itself is well designed, users will perceive the app as more secure.

Second, because our paper is among the first empirical studies of mobile app security, we systematically tested an entire set of MSN designs based on the levels of MSN intrusiveness and disruption in a realistic mobile app context. Furthermore, we examined these MSN designs while users were engaged in a dual-task process. This dual-task experimental environment, using the participants' own devices, makes our MSN designs and testing more realistic, generalizable, and ecologically valid, which are crucial considerations in leading security research [28].

Third, this study identifies an important paradox: the expected MSN design goals may not be achieved due to potential conflicts with the perceptions of mobile users. The common practice of push notifications might actually undermine app security as perceived by the user, not improve it. By designing and examining a set of MSN designs, we found that highly disruptive MSNs can backfire in shaping users' security perceptions of serious security violations.

2. Related work

2.1. Notifications

A *notification* is "a visual cue, auditory signal, or haptic alert generated by an application or service that relays information to a user outside her current focus of attention" ([29], p. 15:2). Today's mobile apps use proactive push notifications to inform users, even inactive ones, about new, unattended messages or events [14] through sounds, vibrations, icons, badges on the app's icons, or auditory-tactile cues, which are core features of many mobile apps. Mobile device users commonly handle many app notifications on a daily basis; Pielot et al. [14] reported an average of 63.5 mobile notifications per day.

Most research on notifications has focused on information workers in desktop environments, where notifications usually have negative effects on completing primary computer tasks. Czerwinski et al. [30] found that it is difficult for users to return to a task after being interrupted, whether by calls, push notifications through instant messages, or interactions with colleagues. Cutrell et al. [20] reported that the negative effect is more pronounced when the task is more cognitively demanding. Leiva et al. [31] found that phone calls interrupting the use of an app significantly increase the time a user spends completing the initial task. De Vries et al. [22] showed that depending on the mental workload, a notification's level of politeness impacts how irritated and disrupted users feel. This could be particularly problematic in a security context, because the processing of serious security threats may involve higher cognitive demands than does the processing of minor threats.

Notifications have clear benefits and costs. Computer system notifications can be delivered to users instantly, thereby reducing their use of cognitive resources to visually scan or repeatedly check information resources [25]. Research has also reported many other benefits of using notifications in a computer-supported work setting, such as improved peer communication [21], heightened awareness of collaboration activities [32], and the relay of application assistance at opportune moments [33]. Again, the negative effects of notifications include irritating interruptions of users' ongoing tasks.

Several studies have examined the trade-off between the disruptions and heightened awareness caused by notifications [25,30,34,35]. Many have also reported innovative solutions to design notification systems based on employing a range of amplitudes [36], frequencies [36–38], vibrations [39], vibration directions [37], intensities [40], and tactile cues [41]. Iqbal and Bailey [25] designed and tested a notification system called Oasis, which aligns notification scheduling with the perceptual structure of user tasks and reduces interruptions of desktop computing tasks. Modic and Anderson [18] examined the various reasons why desktop users often turn off their browser malware warnings, and they provided design guidelines for delivering fewer but more effective security warnings.

2.2. Mobile notifications

Unsurprisingly, as a central feature of today's mobile apps, notifications now play an even more crucial role in proactively informing users of updates, immediate or upcoming events, and system updates [42]. Mobile notifications are typically delivered at the moment data are being sent, whether from games, location-based services [43], or communication-related apps [44]. Depending on the content of notifications, users may have various perceptions of mobile notifications when they are performing tasks in different contexts. If the app is not perceived as useful, mobile notifications can make users irritated enough to cease using it [45]. Conversely, if users consider notifications interesting, entertaining, relevant, and actionable [23], they will be more engaged.

Furthermore, in terms of mobile notification design, visual and auditory cues and vibrations may increase user acceptance. Based on a one-week, in situ (i.e., stationary) study, Pielot et al. [14] reported that regardless of whether or not a mobile device is in silent mode, notifications are typically viewed within minutes. Like desktop notifications, mobile notifications cause cognitive overload, which results in negative emotions and reduced work productivity due to limited resources for focused attention on current tasks [24]. Mashhadi et al. [46] demonstrated that compared to auditory or vibrational cues, visual cues are more effective reminders to return to unread mobile notifications and to quickly deduce the source and importance of these notifications. Moreover, Balebako et al. [47] observed that mobile device users can be irritated by frequent notifications and experience sounds as more irritating than vibrations. Despite the disruptive nature of notifications, users do appreciate the awareness they facilitate [34]. Due to the importance of MSNs, this study focuses on visual cues in notification design, because they are the most effective and common approach for notifying mobile device users.

2.3. Design of MSNs and user perceptions

Because apps are widely used in mobile users' daily routines, the number of security threats to apps is rapidly increasing, including malware, phishing and social engineering, direct attacks by hackers, data communications interception and spoofing, malicious insider actions, and user policy violations [48]. Worse, managing security effectively in mobile environments is a challenge due to a number of technical factors [49]: (1) the mobility and small size of mobile devices, (2) the inability to take advantage of a mobile platform's hardware architecture, (3) obscurity between the platforms (mobile vs. fixed environments) and the underdeveloped understanding of how mobile networks function, (4) the sheer number of mobile attacks, which exhibit a wide variety of attack vectors, and (5) mobile device usability issues. App users are exposed to a mind-numbing barrage of complex security services and mechanisms, which can be confusing for users and result in their underutilization to protect personal data. Again, mobile notifications represent the mainstream technique for increasing user awareness of mobile security issues.

Jøsang and Sanderud [50] suggested making the security services and mechanisms as transparent as possible so that users can easily understand the security process. However, users are often completely oblivious to the security vulnerabilities of their mobile devices, and many users lack an understanding of the security-related services and mechanisms on their mobile devices [12]. Although users have a general sense of the harm to which desktop computers can be subjected due to malware, security vulnerabilities, and so on, they often have no such awareness regarding the vulnerability of their mobile devices [11].

Users desire more fine-grained controls with which to manage their notifications, such as the ability to prioritize notifications depending on their content and source [51]. Similarly, Mashhadi et al. [46] reported that users want to control notification settings in a way that includes different modalities for notifications of varying priorities. However, they also observed that although users are aware of notification controls, they rarely act to change their settings, for two possible reasons: (1) they do not know how to modify their control settings, and (2) they prefer not to go to the trouble of navigating the system settings. The same user behaviors have been associated with security notifications [3,11,17].

Considering the negative attitudes of app users toward MSNs, stakeholders—including mobile OS designers, app designers, and antivirus program companies—face the challenge of how to design user-friendly MSNs without irritating users and thereby causing them to ignore the notifications. However, the academic understanding of mobile app notifications is limited. Consequently, it is crucial to conduct in-depth research to gain a systematic understanding of how the various types of disruptive notifications inform mobile app users' perceived security and their intentions to continue using the app.

Due to the lack of security education and awareness, app users often make the mistake of disregarding security-related notifications. Without a realistic understanding of the threats inherent in mobile platforms and their apps, users form their own, often misguided, perceptions. Ideally, notifications can inform these perceptions, aligning them with security realities, but little is known about how users' security perceptions are formed. In this study, we investigate how app interfaces and the design of MSNs impact users' perceived security and how perceived security, in turn, impacts users' intentions to continue using an app they perceive as secure or insecure.

Because users form perceptions based on the available cues, we examine apps' interface usability as a likely source of the cues used to form security perceptions. The related e-commerce research has shown that website interface quality is an important environmental cue from which users form their security beliefs about websites [52]. Mobile device users have even fewer cues and, therefore, less ability to fully evaluate the security level of the apps on their devices, so they must rely instead on the usability of the app interface to form their security perceptions and their intentions to continue using the app. Given the scarcity of cues available in the mobile environment compared to the traditional desktop environment, it is likely that the mobile app interface design and its usability will exert a stronger influence on the formation of users' perceptions [53]. Jøsang and Sanderud [50] maintained that it is critical to design mobile security interfaces in an intuitive and intelligent way; we thus assume that the mobile app interface and users' perceptions of its usability play important roles in forming users' perceived security.

3. Theoretical model

As discussed, app users often do not have enough knowledge or efficacy to accurately assess the security of a mobile app. They rely on multiple observable design elements of the interface to make their assessment. These observable elements and cues include both app interface usability and the design of MSN.

Consequently, we first focus on mobile app usability to examine users' awareness of and ability to respond to various disruptive MSNs. We draw on the Apple Usability Guidelines [54,55] as a usability foundation for our model, which proposes how the usability of an app interface influences users' security-related perceptions, which in turn influence users' intentions to continue using the app. This portion of our model provides a practice-infused baseline with which to assess the general usability of an app. Likewise, we adopt validated measures of app interface usability from Hoehle and Venkatesh [56], in which the direct visual user interface elements relevant to our study include (1) *user interface graphics*, (2) *user interface input*, (3) *user interface output*, and (4) *user interface structure*.[1]

Given this baseline, we also investigate how disruptive and user-unfriendly MSN designs may decrease users' security perceptions and inhibit sustained usage of the app. Specifically, we explore how MSNs interrupt users' cognitive processing and thus irritate them. This portion

[1] User interface graphics is defined as a user's perception of the effectiveness of the design of a mobile app's graphics; user interface input is defined as a user's perception of whether the app allows easy input of data, such as by providing fingertip-size controls that help the user select functions and menus; user interface output is defined as a user's perception of the effectiveness of the presentation of content in an app interface; user interface structure is defined as a user's perception of the degree to which an app is effectively structured.

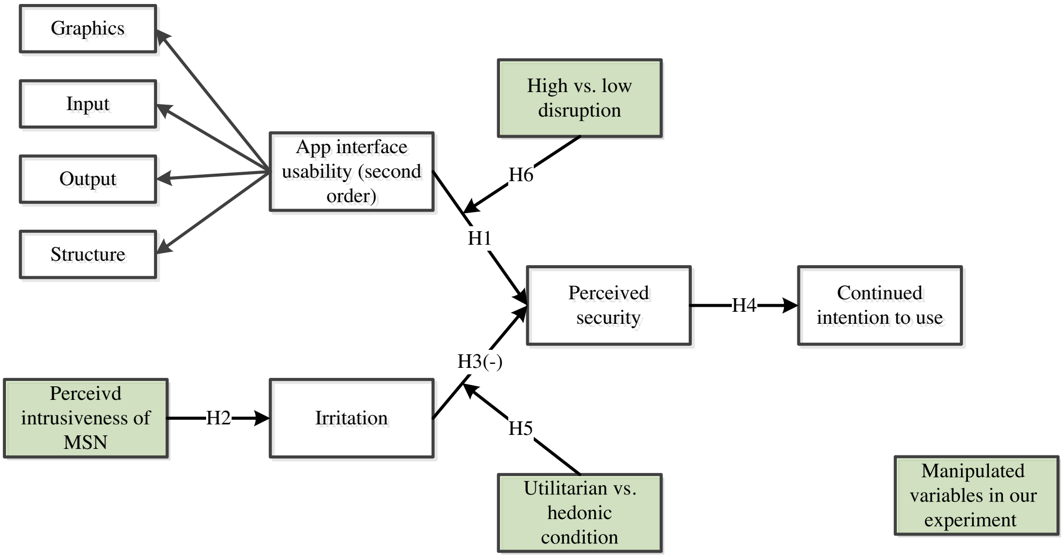

Graphics
Input
Output
Structure
App interface usability (second order)
High vs. low disruption
H6
H1
Perceived security
H4
Continued intention to use
H3(-)
Perceivd intrusiveness of MSN
H2
Irritation
H5
Utilitarian vs. hedonic condition
Manipulated variables in our experiment

Fig. 1. Proposed Theoretical Model and Hypotheses.

of the model builds on the research conducted by McCoy et al. [57], extending their Web-based premises and manipulations to the mobile context. Referencing dual-task interference literature [58,59], we propose that more frequent and disruptive MSNs in the mobile context will lead to more conflicts in processing information, thus causing further user irritation with the app. When notifications interrupt the operations of the mobile device or app and force users to attend to them, they elicit a general sense of dissatisfaction that is likely to have a negative influence on users' continued use of the app. Fig. 1 summarizes our proposed research model, which we explain in more detail in the following section.

3.1. The relationship between app interface usability and perceived security

Research has explored the importance of mobile security in various contexts, such as mobile e-commerce [60], mobile e-banking [61], and communication with mobile devices [62]. However, the antecedents of perceived security have received less attention, in part because, in most situations, it is difficult for mobile users without advanced knowledge of information technology (IT) security to determine whether an app is secure. According to inference theory, when consumers do not have clear knowledge of product quality and value, relevant environmental cues help them form perceptions and make judgments [52]. For instance, in the context of shopping in physical stores, when consumers do not know the exact quality and real value of a product, they rely on environmental cues such as store layout design, store music style, and the number of employees to form their perceptions of quality and price [63]. Similarly, previous research has shown that when users perceive systems as having higher quality of interface design, they perceive the systems themselves as being of higher quality [64]. When visiting websites for the first time, consumers infer quality and trust partially on the basis of website design artifacts and the cobranding of known quality brands or logos [65,66].

Thus, in our context, when users lack expert knowledge, they leverage heuristic cues. For example, e-commerce research has shown that website interface quality is an important influence on consumers' perceptions of the security of the website [52]. If the website interface is well designed, consumers may assume that the website is also willing to invest in website security and regard the website as trustworthy. We extend these findings to the mobile security context by proposing that when users perceive an app as being of high quality, they perceive it in a more favorable light and thus as more secure. This proposition aligns with the cognitive psychological theory of attitude consistency, which emphasizes that individuals tend to align beliefs about the same object (i.e., in this case, the app) to avoid inconsistency [67]. Traditionally, usability has been broadly regarded as "quality of use" and "a quality aspect of products" ([68], p. 481). Thus, when users believe that app interfaces are of high quality, they will infer that other attributes of the apps are likely to have equally high usability, even without any information to corroborate this belief [69]. In summary, an app that is perceived as having high interface usability will be positively related to users' perceived security of the app:

H1. A mobile app's interface usability (consisting of interface graphics, interface input, interface output, and interface structure) is positively related to users' perceived security of the app.

3.2. How intrusive MSN design decreases users' perceived security

Here, we discuss the negative consequences associated with intrusive and user-unfriendly MSN designs. We argue that if an MSN is poorly designed, it not only negatively affects users' security behaviors, but also backfires by decreasing users' security-related perceptions of the app. Next, we explain how the intrusiveness of MSNs arouses the negative emotion of irritation in users, and we then discuss how irritation leads to an attitude change and decreases perceived app security.

3.2.1. The relationship between the intrusiveness of app notifications and user irritation

According to research on dual-task interference, humans have a limited capacity to process information as well as a limited ability to perform multiple tasks simultaneously [58,59,70,71]. Moreover, when multiple tasks require the same type of information processing resources (e.g., reading articles and writing simultaneously), the task interference will be higher [72,73]. Research has suggested that when a secondary task interrupts the performance of a primary task, not only is the person's task performance diminished, but his or her emotions are negatively affected [74]; that is, the person gets irritated.

It has also been found that security notifications/alerts interfere with the flow of IT use, especially in the mobile context [3,16]. In view of the limited cognitive resources humans can devote to information processing, Stuijfzand et al. [75] suggested that the cognitive load of using IT is determined mainly by the amount of information the user needs to process. Further, when the cognitive load is too high, the individual perceives the information as intrusive. Dealing with security notifications requires not only cognitive resources for processing text and graphic information but also hardware resources (from the mobile device) for the presentation of security-related content on a relatively small screen. Thus, an apps' disruptive MSNs conflict strongly with intended tasks, and the message is perceived as intrusive. Worse, as Warner et al. [16] found, when users' typical flow of activity is interrupted by unexpected security messages, which are frequently sent to their mobile devices, users get irritated. Rettie [76] offered similar findings in a study of flow disruptions during Internet use. McCoy et al. [57] investigated the conflict between using e-commerce websites and dealing with disruptive pop-ups and inline ads, and they demonstrated a positive link between online ad intrusiveness and user irritation (in their context, intrusiveness referred to the ad appearing without invitation or in an unwelcome fashion, as perceived by the user; irritation was defined as the user's negative reaction to the ad).

We thus build on the findings of McCoy et al. [57] to predict that when MSNs are perceived as repetitive or unwelcome, they will be perceived as more intrusive. Continual repetition of the same information or the same type of notification, which represents an interferential secondary task, is likely to exhaust the cognitive resources required for information processing. Individuals are likely to perceive this disruption as a meddling force that disturbs their use of the app [77]. Following this logic, we propose that when the user perceives a notification as intrusive, they will experience feelings of irritation. Thus,

H2. The perceived intrusiveness of MSNs is positively related to app user irritation.

3.2.2. The relationship between user irritation and negative outcomes

Building on the psychological research on attitude change [78], we propose that as users' negative emotions regarding apps increase, their intentions or perceptions regarding the mobile devices will also be negatively affected. Irritation toward e-commerce websites and online ads will negatively affect users' value perception and their online shopping behaviors [79]. According to Zuwerink and Devine [80], irritation caused by strong, persuasive messages increases the likelihood of inducing negative attitudes. Thus, when users become irritated by persuasive messages, not only will they be less likely to comply with the message, but they will also be more likely to generate negative affect toward the persuaders. This suggests that in our context, even though app users often understand that the purpose of MSNs is to enhance security and privacy, they still regard MSNs that disrupt their primary tasks as irritating [47]. A large body of research on human–computer interaction has concluded that negative affect toward systems use can have wide-ranging negative consequences for various systems perceptions, including performance, satisfaction, usability, and use [81]. It is then likely that feelings of irritation resulting from app use will negatively influence users' perception of app security: In summary,

H3. The feelings of irritation caused by MSNs are negatively related to users' perceived security of the app.

3.3. The relationship between perceived security and the intention to continue using the app

Users of IT have basic needs for information security. As Belanger et al. [82] pointed out, it is only after users' concerns for information security have been satisfactorily addressed that they will consider using the technology more often. The relationship between perceived security and user intention has been widely tested in various contexts. For instance, e-commerce researchers have found that users with higher perceived security with respect to the technology are more likely to adopt an e-banking system [83], use an e-commerce platform [84], and purchase from a website [85]. Shin [86] found that security beliefs are associated with the intention to use social networking sites. In the mobile context, studies have shown that the perceived security of the technology is related to the use of mobile e-banking [87], the intention to use the app [88], and the intention to use mobile cloud storage services [89]. We thus propose that when users believe an app is secure, they will have strengthened intentions to continue using the app, because they will assume that a negative future event (e.g., a data breach) is unlikely to occur:

H4. Users' perceived security of an app is positively related to intentions to continue using it.

3.4. Moderation effects of utilitarian and hedonic use scenarios

Here, we discuss how utilitarian and hedonic scenarios moderate the influence of irritation on perceived security. In a utilitarian scenario, users are engaged in cognitive tasks such as reading articles and learning [90]. In a hedonic scenario, users are engaged in enjoyable tasks such as playing a mobile game, which leads to higher emotional arousal [91,92]. Moreover, according to Huang and Korfiatis [93], the emotional process often plays a more salient role in determining users' attitude and behavior in a hedonic context than it does in a utilitarian context. Thus, in a hedonic context, people tend to have a stronger cognitive response to emotional elements. In our study, when playing a mobile game (hedonic scenario), users will be in a more highly aroused state than in a utilitarian scenario, and their cognitive assessment of app security at this moment will be more emotionally driven. Consequently, the negative impact of irritation on perceived security will be stronger. By contrast, when reading articles (utilitarian scenario), users are relatively more rational and less emotionally driven than in a hedonic task scenario. Even though the disruptive MSNs irritate them, they are more likely to carefully assess the security level of the app using their existing knowledge and cognitive judgment, and thus less likely to be influenced by irritation. The negative impact of irritation on perceived security will be weaker. We thus hypothesize:

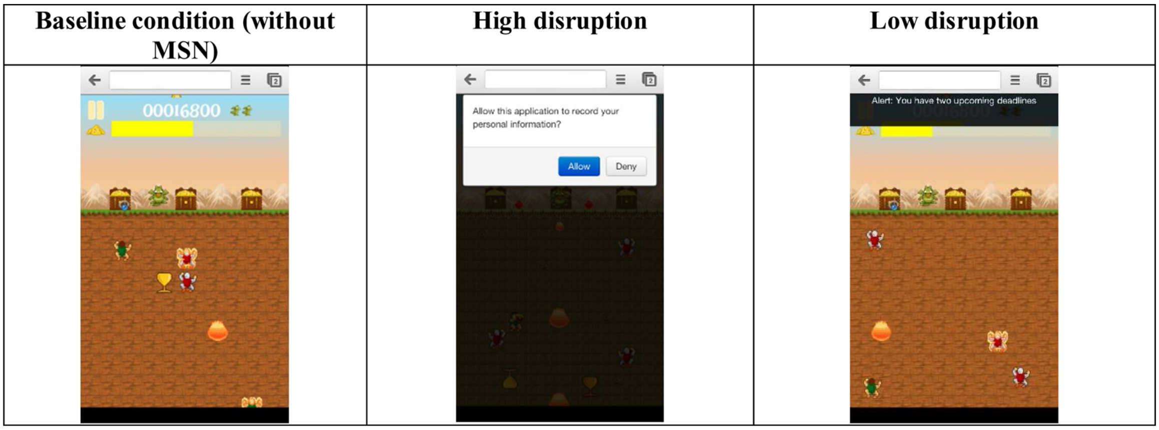
H5. In a hedonic app-use scenario, the negative influence of irritation on perceived security will be stronger than that of a utilitarian app-use scenario.

3.5. Moderation effects of high and low disruption of MSNs

We now explain how the degree of MSN disruption moderates the influence of app usability on perceived security. Details of how MSN disruption is operationalized can be found in Section 4.2.1, Figs. 2 and 3, and Appendix A.

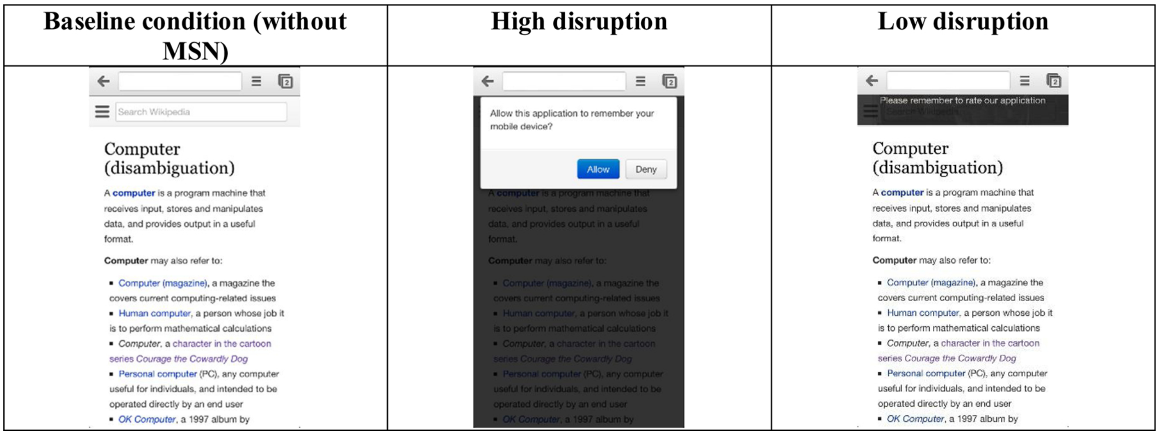
As discussed in Section 3.1, app interface usability has a positive influence on perceived security, because when perceived interface usability is high, users can more effectively interact with the system. Higher interface usability leads to an increase in the flow of use [94]. As a result, users perceive the app as having a higher interface quality when interface usability is high, and this positive perception of the app interface leads to an increase in their security perceptions. However, highly disruptive MSNs may undermine the positive experience brought about by high-quality interface usability. For instance, even when an interface enables effective inputs and outputs, more disruptive MSNs require users to respond to the input and output requests during their app usage. MSNs that entail a high degree of dual-task interference can be disruptive and annoying [94,95]. In the presence of such poorly designed MSNs, even high-quality interface usability cannot result in effective human–computer interactions; such ineffective interaction in turn are likely to decrease users' perceptions of interface quality and perceived security. Thus,

H6. In a high-disruption scenario, the positive influence of app interface usability will be weaker than that in a low-disruption scenario.



Baseline condition (without MSN)	High disruption	Low disruption
	Allow this application to record your personal information? Allow Deny	Alert: You have two upcoming deadlines

Fig. 2. MSNs Displayed in Hedonic Scenarios.



Baseline condition (without MSN)	High disruption	Low disruption
	Allow this application to remember your mobile device? Allow Deny	Please remember to rate our application

Search Wikipedia

Computer (disambiguation)

A **computer** is a program machine that receives input, stores and manipulates data, and provides output in a useful format.

Computer may also refer to:

- Computer (magazine), a magazine the covers current computing-related issues
- Human computer, a person whose job it is to perform mathematical calculations
- *Computer*, a character in the cartoon series *Courage the Cowardly Dog*
- Personal computer (PC), any computer useful for individuals, and intended to be operated directly by an end user
- *OK Computer*, a 1997 album by

Fig. 3. MSNs Displayed in Utilitarian Scenarios.

4. Research methodology

4.1. Study design and pilot testing

We assessed the efficacy of our theoretical model through a controlled survey experiment in a mobile device setting with eight randomized treatment groups (high vs. low MSN intrusiveness, high vs. low MSN disruption, and hedonic vs. utilitarian scenarios) and two control groups without MSNs (hedonic and utilitarian).[2] Both hedonic and utilitarian apps were used, because individuals' behavioral patterns and decision-making may differ between hedonic and utilitarian tasks [92], and we wanted to control for these differences. According to Nasco et al. ([96], p. 989), *utilitarian tasks* are "cognitively driven" and "reasoning based" activities "in which the person's motivations are focused on problem solving"; by contrast, *hedonic tasks* "are primarily characterized by an affective and sensory experience of aesthetic or sensual pleasure, fantasy, or fun." Utilitarian tasks require more cognitive resources, so in this context individuals should be more cognitively driven. Conversely, our hedonic task should lead to higher emotional arousal, so the individuals should be more emotionally driven [96,97]. Given that our study involves both cognitive and affective factors that can drive individuals' perceptions and behaviors, we control for both hedonic and utilitarian conditions through our manipulations. In our study, the cognitive element of app interface usability and the affective element may jointly influence users' security perceptions and continued intention to use; we thus decided to observe the potential differences in utilitarian and hedonic conditions. As suggested by Kim and Sundar ([98], p. 470), adding a manipulation of hedonic/utilitarian tasks can effectively increase the generalizability of the study and the "ecological validity of the experiment."

Following the work of Lowry et al. [90], we conducted a survey experiment that allowed subjects to interact with the mobile application in a naturalistic setting on their own mobile device. Although this approach greatly increases the realism of the methodology, it also greatly diminishes the level of control placed on the experiment and does not allow for strict expectations about the resulting manipulation levels [99–101]. This approach has been used in many information system studies [99,65,100–103]. This methodology allowed us to increase the realism and thus the relevance of the study for the participants, which in this case were college students. Specifically, having the participants use their own devices intensified the relevance of the perceived security of their personal data; this would not have been the case with an impersonal laboratory computer.

We also designed randomly applied treatment conditions with different degrees of MSN intrusiveness (i.e., high vs. low) and notification disruptiveness (see Appendix A) in order to create variance in participants' perceptions of MSN intrusiveness and perceived security and in order to ensure that our findings would be valid under a wide variety of conditions. Information security research based on protection motivation theory has proposed that a message's level of severity affects the likelihood of whether the recipient will or will not respond [104–108]. We thus introduced high- and low-intrusiveness conditions to account for these previously established effects.

To examine our research framework and all hypotheses, we

[2] The two control groups are used to ensure that the general presence of MSNs did not induce any confounding effects beyond the 2*2*2 treatments that influence perceived app security and app use intention.

Table 1
Summary of Experimental Conditions and Number of Participants.

Experimental Conditions		MSN Disruption				Control Group (No MSN)	
		Hedonic App		Utilitarian App		Hedonic App	Utilitarian App
		High	Low	High	Low		
MSN Intrusiveness	**High**	43	25	32	39	17 (not used in SEM analysis)	29 (not used in SEM analysis)
	Low	29	30	39	32		

designed and implemented an app security notification system that can be run by various mobile device platforms. The prototype was built using PHP, JavaScript, HTML5, MySQL, and other mobile-responsive technologies. The mobile app user interfaces were pilot tested with 23 participants to ensure that users experienced the same user interfaces across multiple experimental conditions, while either playing a game or reading a Wikipedia article (see Figs. 2 and 3). Our design of the utilitarian vs. hedonic conditions was consistent with the definitions of utilitarian and hedonic tasks [90] as well as with the common practice adopted by prior research. According to Huang [109] and Hollingsworth and Randolph [110], reading articles and learning are typical utilitarian tasks, whereas playing a game is a typical hedonic task [92,111].

Notably, due to the small screen size of a mobile phone and the different frequencies of MSNs pushed to the users' devices, the captured screenshots often had a slightly different visual appearance, but the primary task backgrounds remained identical while users were scrolling up and down to perform their primary tasks. The MSN system we designed for this study had an automatic function by which it randomly assigned users to different experimental conditions. Based on participant feedback, we improved the system's interface design and usability before running the official controlled experiments.

4.2. Study procedures and conditions

As part of the recruitment process, the participants were first instructed by the researchers about the experiment's procedures in the classroom, and they were then randomly assigned to one of 10 different experimental groups by the experimental server, as shown in Table 1. Not all of our 10 experimental conditions had the same number of participants, for several reasons. First, the server used true random distribution of subjects to conditions; moreover, some subjects had missing or invalid data entries, and some were dropped from the experiment because of Wi-Fi-related issues. We noticed that some subjects became uncomfortable with participating because the MSNs pushed to their mobile phones caused them to perceive a loss of device security. The experiment took participants 15–20 minutes to complete. Before the experiment started, participants were asked to fill out a pre-survey about their demographics, background, and mobile experiences. After they finished the experiment, they were asked to complete an exit questionnaire that assessed the study's major constructs. All participants used mobile phones equipped with our custom-built MSN app, which was designed to manipulate the experimental conditions (see screenshots in Figs. 2 and 3 and Appendix A).

4.2.1. Manipulating the degree of MSN disruption

As shown in Figs. 2 and 3 and Appendix A, a combination of (1) different user interfaces of MSNs and (2) different message contents were designed to manipulate the degrees of MSN disruption. In the highly disruptive treatment condition, participants were exposed to MSNs with high-threat content. They were unable to continue with any other task until they read the entire MSN and then approved or disapproved of the exemption requested by the app. They were then returned to the screen they had been using before the MSN appeared. In the low-disruption condition, an MSN with low-threat content was pushed to participants' mobile phones; these MSNs were minimally inserted (i.e., as a watermarked banner) into the interface but did not obstruct or strongly interfere with the tasks on which the participants were currently working. According to Zijlstra et al. [74], the extent to which a secondary task interrupts a primary task (i.e., the degree of disruption) can be evaluated by the extent to which one can continue performing the primary task. If the disruptiveness is low, one can continue to perform (1) task-related actions and (2) supportive actions associated with the primary task. If the disruptiveness is high, one cannot continue to perform the primary task and must react by performing (3) interruption-handling actions or (4) irrelevant actions.

4.2.2. Manipulating the utilitarian and hedonic use conditions

We also designed two different scenarios for this experiment: a hedonic environment (i.e., an open-source mobile game) and a utilitarian environment (i.e., a Wikipedia article on the subject "computers"). In line with the definitions of utilitarian and hedonic tasks proposed by Nasco et al. [96], Huang [109] and Hollingsworth and Randolph [110] suggested that learning on the basis of reading an article is a typical utilitarian task, and Murray and Bellman [111] suggested that playing a game is a typical hedonic task. We designed our utilitarian and hedonic conditions based on these definitions and on design examples from prior literature. In both scenarios, the participants were exposed to MSNs with different levels of perceived disruptiveness and threat. See Figs. 2 and 3 and Appendix A for screenshots of these treatments.

4.2.3. Manipulating the perceived intrusiveness of MSNs

To manipulate perceived intrusiveness, MSNs were presented to each treatment group of users with a different frequency. Prior research on pop-up ads has suggested that the frequency of pop-up messages has a significant influence on perceived message intrusiveness; thus, this treatment was widely adopted in experimental designs of studies on pop-up ads to manipulate the intrusiveness of pop-up messages [112–115]. In this study, users in the high-intrusiveness groups received an MSN every 40 seconds that reminded them to cope with the potential threats; those in the low-intrusiveness groups received an MSN every 80 seconds.

4.3. Data collection

For the main experimental data collection, we recruited 317 participants from six universities in the United States. The corresponding institutional review boards approved the study, and all participants gave their informed consent to participate. The students' incentive for participating in this study was to earn extra credit in their courses. Our sample consisted of 216 males (68.6 %) and 99 females (31.4 %), and the gender of two participants was unspecified (0.6 %). The average age was 24.3 years (SD = 6.0 years). The average number of years completed at a university was 2.1 (SD =1.0 year). The participants identified themselves either as part-time students (n = 70, 22.2 %), full-time students only (n = 111, 35.1 %), or working full-time while being students (n = 135, 42.7 %), with one unspecified (n = 1, 0.3 %). Among these 317 participants, 271 were assigned to the eight (2*2*2) treatment groups (groups 1–8). The other 46 participants were assigned to the control groups (groups 9–10); they did not receive any MSNs, so they were ineligible to answer questions related to MSNs (e.g., perceived intrusiveness and perceived irritation). The two control groups were set up to ensure that the general presence of MSNs did not induce any confounding effects beyond the 2*2*2 treatments. Specifically, app usability was an important predictor of perceived security and continued intention to use; therefore, a comparison between the eight treatment groups and two control groups indicates that the general presence of MSN itself does not affect perceived app usability (see Appendix C). In this way, the general presence of MSNs in our experiment is intended not to induce any confounding effects on the outcome variables, so all influences on perceived app security and continued intention are induced by our 2*2*2 treatments.

After the main experimental data collection, supplementary data collection was conducted for the purpose of manipulation checks. A total of 101 study participants were recruited, and they participated in the supplementary manipulation check study. The use of a supplementary sample for manipulation checks is a common practice, because it is assumed that effective manipulations can be replicated [116].

All the experimental data collection procedures are presented in Appendix D.

4.4. Measures

After investigating possible validated constructs from the existing theoretical and empirical literature, we obtained the reliable measurement items based on scales from the literature. All construct items were reflectively measured with multiple items on 7-point Likert-type scales. The mobile device user interface constructs were app graphics, user interface input/output, and structure, as adapted from Hoehle and Venkatesh [56]. Notably, that study included six constructs in its instrument development, two of which we did not include (i.e., app design and app utility), because they are not directly related to our mobile security study context. The four constructs we included represented the visual interface design elements of the app. Each of these constructs was a reflective subconstruct of mobile app usability design, and we modeled each of them as separate yet related constructs to explore how the various design elements of the mobile interface influenced our model. The intention-to-continue measurement items were adapted from the unified technology acceptance model [117]. The perceived security construct was based on that of Anderson and Agarwal [118], and the intrusiveness-of-MSN and irritation constructs were adapted from McCoy et al. [57]. The details are presented in Appendix B.

5. Analyses

5.1. Manipulation checks

For the supplementary sample, 101 study participants were recruited and participated in our manipulation check study. They were randomly assigned to the eight (2*2*2) treatment conditions, ensuring an adequate sample size for the supplementary manipulation check.[3] The participants were asked to answer a set of manipulation checks, as shown in Appendix B. Following the standard procedures for manipulation checks, a series of independent samples *t*-tests were conducted [119].

5.1.1. Manipulation check on the MSN disruption treatment

Participants in the manipulation check study were asked to rate the following statement: “When the security warning appeared, I could continue using the app without responding to the warning message” (1 = strongly disagree, 7 = strongly agree) [95]. Based on our manipulation check analysis, we found that the high-MSN-disruption groups (mean = 4.97, SD = 2.01) rated this statement significantly higher than the low-MSN-disruption group (mean = 2.79, SD = 1.75), with t = 5.748 and p = 0.001. These results demonstrated that our manipulation of MSN disruption was successful.

5.1.2. Manipulation check on the utilitarian/hedonic treatment

To check our manipulation of the utilitarian/hedonic treatment, participants were asked to rate the following two statements: when using the app, they were required to complete some tasks (1) for fun (a hedonic purpose) (0 = completely disagree, 100 = completely agree) or (2) for learning (a utilitarian purpose) (0 = completely disagree, 100 = completely agree) [120].

The results of the independent samples *t*-test on this manipulation suggested that participants in the game conditions had a higher hedonic purpose (mean = 68.72, SD = 31.62) than those in the Wikipedia conditions (mean = 40.23, SD = 37.93), with t = 3.828 and p = 0.001. Conversely, participants in the Wikipedia conditions had a higher utilitarian purpose (mean = 73.74, SD = 31.40) than those in the game conditions (mean = 36.50, SD = 34.21), with t = 5.528 and p = 0.001. The above results confirmed that our manipulation of the utilitarian and hedonic app use conditions was successful.

5.1.3. Manipulation check on MSN intrusiveness

The manipulation check on MSN intrusiveness was conducted by comparing the degrees of perceived MSN intrusiveness of the high-intrusiveness and low-intrusiveness groups. The results of the independent samples *t*-test indicate that participants in the high-intrusiveness groups (mean = 5.83, SD = 1.23) reported a significantly higher degree of perceived MSN intrusiveness than those in the low-intrusiveness groups (mean = 4.44, SD = 1.47), with a t = 5.158 and p = 0.001. Thus, we concluded that our manipulation successfully created variance in users' perceived MSN intrusiveness. See Table 2.

5.2. Measurement reliability and validity

Again, participants in the two control groups (group 9 and group 10) did not answer manipulated checks related to MSNs (e.g., perceived intrusiveness and perceived irritation), because they did not receive any MSNs in their experimental conditions. Accordingly, the control group data were not included in the following analysis, which used structural equation modeling (SEM). All the following analyses on manipulation checks and hypothesis testing were conducted using samples in groups 1–8 (271 valid responses), which exactly follow our 2*2*2 manipulations. Data analyses were performed using AMOS 22. This is a common approach to analyzing controlled survey experimental data using SEM estimations [104,121], and it was especially effective in demonstrating the underlying mechanisms of how the treatment variables influence the outcome variables. Before manipulation checks and hypothesis testing, the reliability, convergent validity, and discriminant validity of measures were assessed using AMOS 22. A few measurement items were dropped in the confirmatory factor analysis to improve the measurement validity and model fit. For the final measurement model, the model fit was good: $\chi^2_{391} = 601.200$; $\chi^2/\text{df} = 1.538$; CFI = 0.973; TLI = 0.970; RMSEA = 0.045; PCLOSE = 1.000. Convergent validity was supported by large and standardized loadings for all constructs ($p < .001$) and *t*-values that exceeded statistical significance. Convergent validity was also supported by calculating the ratio of factor loadings to their respective standard errors, which exceeded |10.0| ($p < .001$). The summary statistics of the constructs are presented in Table 3.

Discriminant validity was tested by showing that the measurement model had a significantly better model fit than a competing model with a single latent construct and was better than all other competing models

[3] According to prior literature, 5*N should be an adequate sample size for supplementary manipulation check (N is the number of treatment conditions) [116]. We recruited 101 participants for eight treatment conditions, and each condition had at least 10 participants, which met the 5*N requirement.

Table 2
Summary Results of Manipulation Checks.

Manipulation check on high/low MSN disruption						
	High-disruption group (mean/SD)		Low-disruption group (mean/SD)		*t*-statistic	*p*-value
Degree of disruption	4.97	2.01	2.79	1.75	5.748	0.001
Manipulation check on utilitarian/hedonic treatment						
	Hedonic condition (mean/SD)		Utilitarian condition (mean/SD)		*t*-statistic	*p*-value
Hedonic purpose	68.72	31.62	40.23	37.93	3.828	0.001
Utilitarian purpose	36.50	34.21	73.74	31.40	5.528	0.001
Manipulation check on high/low MSN intrusiveness						
	High-intrusiveness condition (mean/SD)		Low-intrusiveness condition (mean/SD)		*t*-statistic	*p*-value
Perceived intrusiveness	5.83	1.23	4.44	1.47	5.158	0.001

Table 3
Correlations among Latent Constructs.

Constructs	Mean	SD	1	2	3	4	5
1. App interface usability	4.22	1.38	**0.888**				
2. Continued intention to use	3.68	1.88	0.371	**0.911**			
3. Perceived intrusiveness	4.96	1.59	−0.065	−0.107	**0.791**		
4. Perceived security	2.50	1.45	0.400	0.522	−0.313	**0.851**	
5. Irritation	5.04	1.57	−0.118	−0.193	0.713	−0.324	**0.797**

Note: The average variance extracted squared is indicated by the bolded numbers on the diagonal.

in which pairs of latent constructs were joined. The χ^2 differences between the competing models (omitted for the sake of brevity) were significantly larger than that of the original model, as suggested by factor loadings, modification indices, and residuals [122]. In summary, these tests confirmed convergent and discriminant validities.

Construct reliability was assessed using Cronbach's α. All measures exceeded 0.70 (see Table 4), suggesting strong reliability. Reliability was also supported because the average variance extracted [123] exceeded 0.50 for all factors. Furthermore, common method bias was assessed via procedures outlined in Podsakoff et al. [124], indicating that common method bias was not a concern for this study.[4]

5.3. Hypothesis testing for the direct effects in H1–H4

We first tested the baseline model, which included only the direct relationships (H1–H4). The structural model was assessed using AMOS 22. Common fit indices showed that the model fit was acceptable: $\chi^2_{394} = 610.085$; $\chi^2/\text{df} = 1.548$; CFI = 0.972; TLI = 0.969; RMSEA = 0.045; PCLOSE = 1.000. All control variables (age, gender, level of education, work status, Internet experience, and previous privacy victim status) were nonsignificant predictors of our dependent variables. Fig. 4 shows the results of the baseline model test, which are detailed in Table 5. As indicated in Fig. 4 and Table 5, the model explained approximately 51.4 % of variance in irritation, 24.4 % of variance in perceived security, and 28.1 % of variance in continued intention to use.

First, we confirmed that the perceived security of the mobile app was influenced by users' cognitive evaluation of the mobile interface design (β = 0.380, $p < .001$, H1 supported). With a better-designed interface and improved interface usability, users perceived the app as more secure. Second, we found that user-unfriendly MSNs decreased perceived security due to the negative emotion of irritation. Perceived MSN intrusiveness significantly influenced irritation (β = 0.717, $p < .001$, H2 supported), which in turn resulted in a decrease in the perceived security of the app (β = -0.296, $p < .001$, H3 supported). Finally, perceived app security was a crucial determinant of continued intention to use the app (β = 0.530, $p < .001$, H4 supported).

Table 4
Construct Reliability and Validity Scores.

Construct	Cronbach's α	AVE	CR
1. App interface usability	0.933	0.788	0.937
2. Continued intention to use	0.861	0.830	0.951
3. Perceived intrusiveness	0.890	0.625	0.868
4. Perceived security	0.910	0.725	0.913
5. Irritation	0.964	0.635	0.873

5.4. Hypothesis testing for moderation effects

Next, we tested the contingent factors that moderate the influence of interface usability and MSN-induced irritation on perceived security (H5 and H6).

5.4.1. Contingent effect of utilitarian and hedonic scenarios

H5 suggested that the negative effect of irritation is more pronounced in hedonic scenarios than in utilitarian scenarios. To test this hypothesis, we performed the multigroup analysis in AMOS (chi-square test) as well as the differences-in-slopes test suggested by Chin [125]. The multigroup analysis results are summarized in Table 6. The χ^2 differences between the constrained models (for the two subgroups, the coefficient of the relationship irritation→perceived security was constrained to be equal) were significantly larger than that of the original unconstrained model, suggesting that the effect proposed in H3 was

[4] For the sake of brevity, these details have been omitted and are available from the authors upon request.

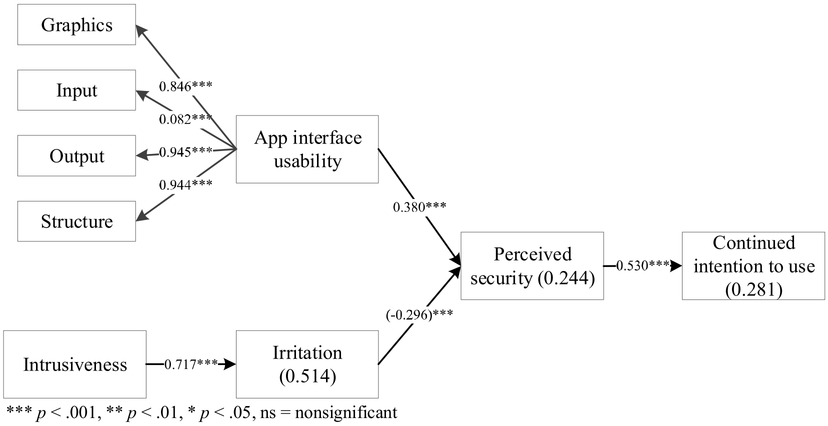


Fig. 4. Hypothesis Testing for H1–H4.
*** $p < .001$, ** $p < .01$, * $p < .05$, ns = nonsignificant.

Table 5
Hypothesis Testing for H1–H4.

Hypothesis	β	S.E.	*t*	*p*	Support?
H1: Mobile app interface usability → Perceived security	0.380	0.065	5.993	< 0.001	Yes
H2: Perceived intrusiveness of MSN → Irritation	0.717	0.096	9,280	< 0.001	Yes
H3: Irritation → Perceived security	−0.296	0.057	−4.741	< 0.001	Yes
H4: Perceived security → Continued intention to use	0.530	0.084	8.358	< 0.001	Yes

Table 6
Multigroup Analysis for Utilitarian and Hedonic Scenarios.

Relationship	Unstandardized coefficients (in unconstrained model)	
	Utilitarian scenario	Hedonic scenario
H1: Mobile app interface usability → Perceived security	0.44	0.32
H2: Perceived intrusiveness of MSN → Irritation	0.96	0.91
H3: Irritation → Perceived security	**−0.10**	**−0.51**
H4: Perceived security → Continued intention to use	0.83	0.65

Parameter constraint: coefficients in H3 are equal across utilitarian and hedonic scenarios.
$\Delta\chi^2/\Delta df = 17.570, p < .001$. The influence of irritation → perceived security is significantly different across utilitarian and hedonic scenarios.

significantly different across the utilitarian and hedonic scenarios.

Next, we performed the differences-in-slopes test based on Chin [125] using the formula below:

$$t = \frac{Path_{sample\_1} - Path_{sample\_2}}{\left[\sqrt{\frac{(m-1)^2}{(m+n-2)} * S.E._{sample1}^2 + \frac{(n-1)^2}{(m+n-2)} * S.E._{sample2}^2}\right] * \left[\sqrt{\frac{1}{m} + \frac{1}{n}}\right]}$$

The results summarized in Table 7 indicate that the negative influence of irritation on perceived security was stronger in hedonic scenarios; thus, H5 was supported.

Table 7
Differences-in-Slopes Test for Utilitarian and Hedonic Scenarios.

	Hedonic scenario	Utilitarian scenario
Sample Size	129	142
Regression Weight	−0.51	−0.10
Standard Error (S.E.)	0.065	0.068
t-statistic	4.355	
p-value (two-tailed)	< 0.001	

Table 8
Multigroup Analysis for High- and Low-Disruption Conditions.

Relationship	Unstandardized coefficients (in unconstrained model)	
	High disruption	Low disruption
H1: Mobile app interface usability → Perceived security	**0.30**	**0.54**
H2: Perceived intrusiveness of MSN → Irritation	1.04	0.85
H3: Irritation → Perceived security	−0.30	−0.26
H4: Perceived security → Continued intention to use	0.70	0.80

Parameter constraint: coefficients in H1 are equal across utilitarian and hedonic scenarios.
$\Delta\chi^2/\Delta df = 4.371$, p = .037. The influence of interface usability → perceived security is significantly different across high- and low-disruption conditions.

Table 9
Differences-in-Slopes Test for High- and Low-Disruption Conditions.

	High disruption	Low disruption
Sample Size	145	126
Regression Weight	0.30	0.54
Standard Error (S.E.)	0.089	0.072
t-statistic	2.064	
p-value (two-tailed)	0.040	

5.4.2. *Contingent effect of high/low disruption of MSNs*

We then tested H6 using the procedures described in the previous section, and the results are listed in Tables 8 and 9. H6 was supported, because significant differences were found in the coefficients for high- and low-disruption conditions. Along with the increase in MSN disruption, the positive influence of interface usability on perceived security was weakened.

6. Discussion

Daily use of mobile devices is becoming a common way of life throughout the world. Although substantial research has investigated the adoption of mobile apps, little research has focused on how to make app users aware of the security issues inherent in mobile apps. Given the increasing pervasiveness of app security issues, this is particularly problematic. Although most users are aware of how viruses, phishing attacks, and other malware can affect their personal computers and laptops, few are aware of similar threats for mobile apps, know how to cope with them, or take them seriously. Worse, users routinely ignore security push notifications from apps, which are essential to improving users' app security. Users also tend to find these notifications irritating, which may negatively influence their intentions to use the app.

Accordingly, the purpose of this study is to explain and predict how mobile app interface usability and the design of MSNs influence users' perceived security and their intentions to continue using apps. We conducted a set of survey experiments in which 317 smartphone users were exposed to different levels of security-related notifications and various levels of security-related threats on their own devices. Our results indicate that (1) interface usability and perception of MSN designs are two important determinants of perceived security of the mobile app, (2) perceived mobile app security is positively associated with continued intention to use the mobile app, and (3) the influences of interface usability and irritation on perceived security are contingent on the context of use (utilitarian/hedonic) and the MSN type (high disruption/low disruption).

6.1. Contributions to research, theory, and practice

Our first key contribution is to explain the influence of MSNs on users' security perception and continued use intentions. During the experiment, we were able to verify the existence of user irritation caused by the MSNs while users were performing a primary task. Our findings also challenge the current literature, because they indicate that our mobile users' decision-making process regarding whether they would continue to use the mobile app was not easily influenced by their negative emotions caused by the disruptive MSNs. This suggests that our participants (and possibly today's mobile users more generally) were more rational than most of the current literature claims. We thus call for research that more accurately characterizes today's mobile user behaviors, especially with respect to mobile security.

We validated our proposition that the disruptive effects of MSNs can backfire and decrease users' perceived security. This is a counterintuitive and novel notion that requires further study. That is, we found that if MSNs are not properly designed, they can reduce users' security perceptions. In this study, we explain the antecedents of users' perceived security of apps, considering that most users do not have the professional knowledge with which to accurately evaluate security levels. We thus conclude that if designers can more clearly present notification information and increase the ease of information entry, app users' security perceptions will be enhanced. Given the scant empirical research on mobile security, no study to date has reported antecedents that increase users' perceived security of mobile devices or their accompanying apps. Moreover, this is the first empirical study to systematically examine whether MSNs designed to disrupt the user decrease perceived security.

Our second key contribution is to explain the effect of mobile app usability on perceived app security and continued intention to use the app. The extant security literature has a major research gap concerning how mobile device users evaluate their apps in terms of perceived security. In this study, we found that when users lack sufficient knowledge to accurately evaluate app security, their assessments rely heavily on explicit heuristic cues. We found that app users evaluate mobile app security based on perceived app interface usability. Much research has demonstrated the importance of perceived ease of use and perceived usefulness with respect to continued use; however, the influence of app interface usability and MSN design on mobile security perceptions had not been systematically explored prior to this study. The latter finding is particularly interesting, because evidence from other studies shows that app users have low security awareness and routinely dismiss MSNs. However, despite this lack of awareness and attention to notifications, our results show that if users merely perceive the app as secure, they will be more likely to continue using it. Given the lack of user training on security, app designers could focus instead on environmental cues (such as usability design) to increase security perceptions, because users are most likely to rely on such cues to make credibility and trust assessments. If our results hold, practitioners should focus their usability interaction design on four key dimensions: graphics, input, output, and structure.

As a third contribution, we extended our findings by comparing the coefficients of different conditions (hedonic vs. utilitarian scenarios and high- vs. low-disruption notifications). The different degrees of threat violation and message intrusiveness can effectively induce different degrees of dual-task interference and can create sufficient variation in mobile app users' emotional states (e.g., irritation) and security-related perceptions. As a result, we were able to observe the differences in users' cognitive and emotional responses to MSNs when they were subjected to different degrees of disruption. Moreover, we found that the negative impact of intrusive MSNs and the negative emotions caused by dual-task interference are more pronounced in hedonic scenarios than in utilitarian scenarios. This comparison not only increases the generalizability of our conclusions but also provides insights into task–technology fit that enhance the understanding of MSN design.

To illustrate, although MSNs are important in fostering app users' security awareness, when MSNs interrupt the typical workflow of app users, they feel even less secure; our results show a decrease in perceived security. By examining how users perceived low- and high-disruption notifications across different app usage scenarios, we developed a practical guideline of focusing on low-disruption notifications rather than high- or no-disruption notifications. Given the predominance of highly disruptive notifications that require an action from the user to proceed, this finding has strong practical implications, because users perceive such notifications as indications that the app is less secure. Even if the notification focuses on how the app is blocking a malicious attempt or attack, users still experience a decrease in perceived security, which then further reduces their intention to continue using the app. Thus, app designers should focus on conveying information through MSNs by means of a less disruptive method, which would increase users' perceived security and support their intention to continue using the app. As an example, MSNs with high threats should be pushed less frequently to minimize the disruptions to users' primary tasks. Instead of fully controlling the entire smartphone screen to disable users' current primary tasks, we suggest using less-intrusive visual or audio cues (such as highlights, alarm tones, or similar "nudges").

6.2. Limitations and future research

Our study had several limitations that suggest promising research opportunities. First, the generalizability of our conclusions was limited by our use of students and by our experimental design. On the one hand, a student sample was acceptable for this study because students are heavy app users. We also followed recent guidelines for enhancing *ecological validity* (which is distinct from generalizability and crucial to security research) [28] by having the participants use their own devices, which made the security concerns, threats, and irritation more realistic than using laboratory devices. On the other hand, differences may exist between students, professionals, and older consumers in terms of security awareness, perceived security, and what constitutes an irritating disruption. In fact, given that millennials and post-millennials are the most tech-savvy generation and the generation most prone to multitasking, it is possible that the more disruptive notifications cause them more irritation than other populations, but this has not been empirically studied.

Second, we adopted an experimental approach that engaged app users in several different scenarios. Unsurprisingly, the study results were partially influenced by the specific app and notification messages we provided. Our experiments could be substantially improved by the addition of a user attention check, which would ask participants to answer questions about whether they noticed any disruptions during the experimental period. This could be particularly useful, because users in low-violation conditions in the current study did not have to act in response to the MSNs pushed to their mobile phones.

In addition, to enhance ecological validity, it is also crucial to expand this study into business environments in future research [28]. This would fit naturally with our study, because the bring-your-own-device (BYOD) work trend poses a threat to organizational security [9]. Many other aspects of security could be explored, such as mobile security policy, offensive security, network security architecture, intrusion detection and prevention systems, honeypots, and data breaches.

Although this study compared high- and low-security violation conditions, high- and low-disruption notifications, and hedonic and utilitarian conditions, future research should examine more individual-level factors that could influence the outcomes. Such factors could include individual traits, cultural differences, self-efficacy, security awareness, and different types of mobile devices. Given that we have shown the importance of irritation in this setting, we surmise that other recent research on the further role of positive psychology [105], and positive and negative emotions in security settings [126,127], could be particularly useful to consider. This is particularly compelling in our context as emotions and system design interact, and these can affect security perceptions (and subsequent behaviors) positively or negatively.

Likewise, future research should explore whether notification type corresponds to the degree of threat that is broadcast via the notification and whether outcomes improve if users can better assess the level of threats. For example, highly threatening notifications may produce better outcomes if they are highly disruptive, even though users find such disruptiveness irritating. Similarly, it might be better for low-threat notifications to be less disruptive. This implies that differentiating and customizing the design of MSNs in various contexts may improve the design of today's apps.

Our findings also demonstrated the importance of MSNs in increasing users' security awareness. This idea could be expanded into mobile security training that uses various security scenarios to teach app users to make sound decisions regarding the use of their mobile devices in the workplace. This practice may be beneficial to businesses as well as individual app users.

Finally, we showed that app interface design and security-related notifications influence users' perceived security. Thus, future research could refine apps or MSNs not only to enhance mobile security interface design but also to increase user security awareness. Furthermore, we cannot ignore the fact that poorly designed notifications can cause user irritation, which negatively affects users' perceived security. To advance knowledge in this area, we call for MSN-design research that further differentiates levels of MSN intrusiveness by examining the designs of malicious and regular low-intrusive MSNs and their impacts on user behaviors. Thus, researchers should carefully consider the design of MSNs customized to different mobile devices, different users, and different security contexts [15].

7. Conclusion

In this study, we proposed that two important app design artifacts strongly influence users' perceived security and intentions to continue using the app: mobile app interface usability and the design of MSNs. Drawing on the literature on dual-task interference and attitude change, we explored how negative perceptions caused by disruptive designs can interfere with the flow of activity during app use and decrease perceived security and the intention to continue using the app. Our model's results provide an opportunity for future research to explore the underlying mechanisms of and influences on perceived security in different situations. Moreover, future research could investigate the security compliance and coping behaviors associated with security-related designs, which this study did not address.

Acknowledgements

We would like to express our sincere appreciation to the constructive feedback, suggestions and edits from the editor-in-chief, associate editor, and the three anonymous reviewers. We are also thankful to all our study participants' time and efforts to participate in our study, and great colleagues who significantly helped with the recruitment of our study participants in multiple US institutions for the project. This work was partially supported by the University of South Carolina Grant (Grant No. 80002838).

Appendix A. Supplementary data

Supplementary material related to this article can be found, in the online version, at doi:https://doi.org/10.1016/j.im.2019.103235.

References

[1] A. Goode, Managing mobile security: How are we doing? Netw. Secur. 2010 (2) (2010) 12–15.
[2] M.J. Keith, S.C. Thompson, J. Hale, P.B. Lowry, C. Greer, Information disclosure on mobile devices: re-examining privacy calculus with actual user behavior, Int. J. Hum. Stud. 71 (12) (2013) 1163–1173.
[3] A.P. Felt, M. Finifter, E. Chin, S. Hanna, D. Wagner, A survey of mobile malware in the wild, 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, Chicago, IL: ACM, 2011, pp. 3–14.
[4] Y. Zhou, Z. Wang, W. Zhou, X. Jiang, Hey, you, get off of my market: detecting malicious apps in official and alternative Android markets, 19th Network and Distributed System Security Symposium (NDSS'12), San Diego, CA: Internet Society, 2012.
[5] A. Zacks, Malware Statistics, Trends and Facts in 2019, Retrieved April 13, 2019, from (2018) https://www.safetydetective.com/blog/malware-statistics/.
[6] R. Sobers, 60 Must-Know Cybersecurity Statistics for 2019, Retrieved April 13, 2019, from (2019) https://www.varonis.com/blog/cybersecurity-statistics/.
[7] D. Harborth, M. Hatamian, W.B. Tesfay, K. Rannenberg, A two-pillar approach to analyze the privacy policies and resource access behaviors of mobile augmented reality applications, January 8-11, Paper Presented at the Proceedings of the 52nd Hawaii International Conference on System Sciences, Maui, HI, 2019.
[8] J. Rouse, Mobile devices – the most hostile environment for security? Netw. Secur. 2012 (3) (2012) 11–13.
[9] S. Allam, S.V. Flowerday, E. Flowerday, Smartphone information security awareness: a victim of operational pressures, Comput. Secur. 42 (May) (2014) 56–65.
[10] J. Lu, C. Liu, C.-S. Yu, K. Wang, Determinants of accepting wireless mobile data services in China, Inf. Manag. 45 (1) (2008) 52–64.
[11] A. Mylonas, A. Kastania, D. Gritzalis, Delegate the smartphone user? Security awareness in smartphone platforms, Comput. Secur. 34 (May) (2013) 47–66.
[12] P. McDaniel, W. Enck, Not so great expectations: why application markets haven't failed security, IEEE Secur. Priv. 8 (5) (2010) 76–78.
[13] I. Warren, A. Meads, S. Srirama, T. Weerasinghe, C. Paniagua, Push notification mechanisms for pervasive smartphone applications, IEEE Pervasive Comput. 13 (2) (2014) 61–71.
[14] M. Pielot, K. Church, Rd. Oliveira, An in-situ study of mobile phone notifications, Proceedings of the 16th International Conference on Human-Computer Interaction

with Mobile Devices and Services, Toronto, ON, Canada: ACM, 2014, pp. 233–242.
[15] S. Ochs, Meet the company that's making push notifications smarter, Macworld 31 (6) (2014) 30.
[16] J.H.R. Warner, S. Miller, K. Jennings, H. Lundsgaarde, P. Pincetl, E.N. Robinson Jret al., Clinical event management using push technology—implementation and evaluation at two health care centers, Proceedings of the AMIA Symposium, American Medical Informatics Association, 1998, pp. 106–110.
[17] P.G. Kelley, S. Consolvo, L.F. Cranor, J. Jung, N. Sadeh, D. Wetherall, A conundrum of permissions: installing applications on an Android smartphone, Financial Cryptography and Data Security: Lecture Notes in Computer Science, Springer, Heidelberg, Germany, 2012, pp. 68–79.
[18] D. Modic, R. Anderson, Reading this may harm your computer: the psychology of malware warnings, Comput. Hum. Behav. 41 (December) (2014) 71–79.
[19] B.P. Bailey, S.T. Iqbal, Understanding changes in mental workload during execution of goal-directed tasks and its application for interruption management, ACM Trans. Comput. Interact. 14 (4) (2008) 1–28.
[20] M. Cutrell, E. Czerwinski, E. Horvitz, Notification, disruption, and memory: effects of messaging interruptions on memory and performance, in: M. Hirose (Ed.), Proceedings of Human-Computer Interaction: INTERACT'01: IFIP TC. 13 International Conference on Human-Computer Interaction, Tokyo, Japan: IOS Press, 2001, pp. 263–269.
[21] M. Czerwinski, E. Horvitz, An investigation of memory for daily computing events, in: X. Faulkner, J. Finlay, F. Détienne (Eds.), People and Computers XVI - Memorable Yet Invisible: Proceedings of HCI 2002, London: Springer London, 2002, pp. 229–245.
[22] R.A.J. De Vries, M. Lohse, A. Winterboer, F.C.A. Groen, V. Evers, Combining social strategies and workload: a new design to reduce the negative effects of task interruptions, CHI' 13 Extended Abstracts on Human Factors in Computing Systems, Paris, France: ACM, 2013, pp. 175–180.
[23] J.E. Fischer, N. Yee, V. Bellotti, N. Good, S. Benford, C. Greenhalgh, Effects of content and time of delivery on receptivity to mobile interruptions, Proceedings of the 12th International Conference on Human Computer Interaction with Mobile Devices and Services, Lisbon, Portugal: ACM, 2010, pp. 103–112.
[24] D. Garlan, D.P. Siewiorek, A. Smailagic, P. Steenkiste, Project aura: toward distraction-free pervasive computing, IEEE Pervasive Comput. 1 (2) (2002) 22–31.
[25] S.T. Iqbal, B.P. Bailey, Oasis: a framework for linking notification delivery to the perceptual structure of goal-directed tasks, ACM Trans. Comput. Interact. 17 (4) (2010) 1–28.
[26] M. Wiberg, S. Whittaker, Managing availability: supporting lightweight negotiations to handle interruptions, ACM Trans. Comput. Interact. 12 (4) (2005) 356–387.
[27] G. Dhillon, T. Oliveira, S. Susarapu, M. Caldeira, Deciding between information security and usability: developing value based objectives, Comput. Hum. Behav. 61 (August) (2016) 656–666.
[28] P.B. Lowry, T. Dinev, R. Willison, Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda, Eur. J. Inf. Syst. 26 (6) (2017) 546–563.
[29] S.T. Iqbal, B.P. Bailey, Effects of intelligent notification management on users and their tasks, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Florence, Italy: ACM, 2008, pp. 93–102.
[30] M. Czerwinski, E. Horvitz, S. Wilhite, A diary study of task switching and interruptions, Proceedings of the Conference on Human Factors in Computing Systems, Vienna, Austria: ACM, 2004, pp. 175–182.
[31] L. Leiva, M. Böhmer, S. Gehring, A. Krüger, Back to the app: the costs of mobile application interruptions, Proceedings of the 14th International Conference on Human-Computer Interaction with Mobile Devices and Services, San Francisco, CA: ACM, 2012, pp. 291–294.
[32] L. Dabbish, R.E. Kraut, Controlling interruptions: awareness displays and social motivation for coordination, Proceedings of the 2004 ACM Conference on Computer Supported Cooperative Work, Chicago, IL, 2004, pp. 182–191.
[33] P. Maes, Agents that reduce work and information overload, Commun. ACM 37 (7) (1994) 30–40.
[34] S.T. Iqbal, E. Horvitz, Notifications and awareness: a field study of alert usage and preferences, Proceedings of the 2010 ACM Conference on Computer Supported Cooperative Work, Savannah, GA: ACM, 2010, pp. 27–30.
[35] B.C. Lin, J.M. Kain, C. Fritz, Don't interrupt me! An examination of the relationship between intrusions at work and employee strain, Int. J. Stress Manag. 20 (2) (2013) 77–94.
[36] J. Ryu, J. Jung, S. Choi, Perceived magnitudes of vibrations transmitted through mobile device, Symposium on Haptic Interfaces for Virtual Environments and Teleoperator Systems 2008, Reno, NV, 2008, pp. 139–140.
[37] J. Hwang, W. Hwang, Vibration perception and excitatory direction for haptic devices, J. Intell. Manuf. 22 (1) (2009) 17–27.
[38] H.-Y. Yao, D. Grant, M. Cruz, Perceived vibration strength in mobile devices: the effect of weight and frequency, IEEE Trans. Haptics 3 (1) (2010) 56–62.
[39] B. Saket, C. Prasojo, Y. Huang, S. Zhao, Designing an effective vibration-based notification interface for mobile phones, Proceedings of the 2013 Conference on Computer Supported Cooperative Work, San Antonio, TX: ACM, 2013, pp. 1499–1504.
[40] T.L. White, The Perceived Urgency of Tactile Patterns: Human Research and Engineering Directorate, Last updated Army Research Laboratory, 2011 ARL-TR-5557. Retrieved.
[41] H. Qian, R. Kuber, A. Sears, Towards identifying distinguishable tactons for use with mobile devices, Proceedings of the 11th International ACM SIGACCESS Conference on Computers and Accessibility, Pittsburgh, PA: ACM, 2009, pp. 257–258.
[42] D. Weber, A.S. Shirazi, N. Henze, Towards smart notifications using research in the large, Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct, Copenhagen, Denmark: ACM, 2015, pp. 1117–1122.
[43] J.W. Streefkerk, M.Pv. Esch-Bussemakers, M.A. Neerincx, Field evaluation of a mobile location-based notification system for police officers, Proceedings of the 10th International Conference on Human Computer Interaction with Mobile Devices and Services, Amsterdam, The Netherlands: ACM, 2008, pp. 101–108.
[44] Y.-J. Chang, J.C. Tang, Investigating mobile users' ringer mode usage and attentiveness and responsiveness to communication, Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services, Copenhagen, Denmark: ACM, 2015, pp. 6–15.
[45] A.P. Felt, S. Egelman, D. Wagner, I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns, Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, Raleigh, NC: ACM, 2012, pp. 33–44.
[46] A. Mashhadi, A. Mathur, F. Kawsar, The myth of subtle notifications, Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication, Seattle, WA: ACM, 2014, pp. 111–114.
[47] R. Balebako, J. Jung, W. Lu, L.F. Cranor, C. Nguyen, 'Little brothers watching you': raising awareness of data leaks on smartphones, Proceedings of the Ninth Symposium on Usable Privacy and Security, Newcastle, UK: ACM, 2013, pp. 1–14.
[48] J. Friedman, D.V. Hoffman, Protecting data on mobile devices: a taxonomy of security threats to mobile computing and review of applicable defenses, Inf. Knowl. Syst. Manage. 7 (1/2) (2008) 159–180.
[49] J. Oberheide, F. Jahanian, When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments, Proceedings of the Eleventh Workshop on Mobile Computing Systems and Applications, Annapolis, MD: ACM, 2010, pp. 43–48.
[50] A. Jøsang, G. Sanderud, Security in mobile communications: challenges and opportunities, Australian Computer Society, Proceedings of the Australasian Information Security Workshop Conference on ACSW Frontiers 2003, Vol. 21 2003, pp. 43–48.
[51] A.S. Shirazi, N. Henze, T. Dingler, M. Pielot, D. Weber, A. Schmidt, Large-scale assessment of mobile notifications, Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems, Toronto, Ontario, Canada: ACM, 2014, pp. 3055–3064.
[52] H.H. Chang, S.W. Chen, Consumer perception of interface quality, security, and loyalty in electronic commerce, Inf. Manag. 46 (7) (2009) 411–417.
[53] R.A. Botha, S.M. Furnell, N.L. Clarke, From desktop to mobile: examining the security experience, Comput. Secur. 28 (3) (2009) 130–137.
[54] Apple Inc, User Experience Guidelines, Retrieved June 4, 2014, from (2013) https://developer.apple.com/library/mac/documentation/userexperience/conceptual/applehiguidelines/UEGuidelines/UEGuidelines.html.
[55] V. Venkatesh, V. Ramesh, Web and wireless site usability: understanding differences and modeling use, MIS Q. 30 (1) (2006) 181–206.
[56] H. Hoehle, V. Venkatesh, Mobile application usability: conceptualization and instrument development, MIS Q. 39 (2) (2015) 435–472.
[57] S. McCoy, A. Everard, P. Polak, D.F. Galletta, An experimental study of antecedents and consequences of online ad intrusiveness, Int. J. Hum. Interact. 24 (7) (2008) 672–699.
[58] D. Navon, D. Gopher, On the economy of the human-processing system, Psychol. Rev. 86 (3) (1979) 214–255.
[59] H. Pashler, Dissociations and dependencies between speed and accuracy: evidence for a two-component theory of divided attention in simple tasks, Cogn. Psychol. 21 (4) (1989) 469–514.
[60] A.K. Ghosh, T.M. Swaminatha, Software security and privacy risks in mobile e-commerce, Commun. ACM 44 (2) (2001) 51–57.
[61] R. Schierholz, T. Laukkanen, Internet vs mobile banking: comparing customer value perceptions, Bus. Process. Manag. J. 13 (6) (2007) 788–797.
[62] T. Kindberg, A. Sellen, E. Geelhoed, Security and trust in mobile interactions: a study of users' perceptions and reasoning, in: N. Davies, E. Mynatt, I. Siio (Eds.), UbiComp 2004: Ubiquitous Computing, Vol. 3205 Springer, Heidelberg, Germany, 2004, pp. 196–213.
[63] J. Baker, A. Parasuraman, D. Grewal, G.B. Voss, The influence of multiple store environment cues on perceived merchandise value and patronage intentions, J. Mark. 66 (2) (2002) 120–141.
[64] D. Cyr, M. Head, A. Ivanov, Design aesthetics leading to m-loyalty in mobile commerce, Inf. Manag. 43 (8) (2006) 950–963.
[65] P.B. Lowry, A. Vance, G. Moody, B. Beckman, A. Read, Explaining and predicting the impact of branding alliances and web site quality on initial consumer trust of e-commerce web sites, J. Manag. Inf. Syst. 24 (4) (2008) 199–224.
[66] P.B. Lowry, D.W. Wilson, W.L. Haig, A picture is worth a thousand words: source credibility theory applied to logo and website design for heightened credibility and consumer trust, Int. J. Hum. Interact. 30 (1) (2014) 63–93.
[67] M.M. Thompson, M.P. Zanna, The conflicted individual: personality-based and domain-specific antecedents of ambivalent, J. Pers. 63 (2) (1995) 259–288.
[68] M. Hassenzahl, The effect of perceived hedonic quality on product appealingness, Int. J. Hum. Interact. 13 (4) (2001) 481–499.
[69] J.W. Alba, J.W. Hutchinson, Dimensions of consumer expertise, J. Consum. Res. 13 (4) (1987) 411–454.
[70] S. Jeuris, J.E. Bardram, Dedicated workspaces: faster resumption times and reduced cognitive load in sequential multitasking, Comput. Hum. Behav. 62 (September) (2016) 404–414.
[71] J. Srivastava, Media multitasking performance: role of message relevance and formatting cues in online environments, Comput. Hum. Behav. 29 (3) (2013)

888–895.
[72] R.S. McCann, J.C. Johnston, Locus of the single-channel bottleneck in dual-task interference, J. Exp. Psychol. Hum. Percept. Perform. 18 (2) (1992) 471–484.
[73] C.D. Wickens, Processing Resources in Attention, Dual Task Performance, and Workload Assessment, Defense Technical Information Center, Fort Belvoir, VA, 1981.
[74] F.R.H. Zijlstra, R.A. Roe, A.B. Leonora, I. Krediet, Temporal factors in mental work: effects of interrupted activities, J. Occup. Organ. Psychol. 72 (2) (1999) 163–185.
[75] B.G. Stuijfzand, M.F. van der Schaaf, F.C. Kirschner, C.J. Ravesloot, A. van der Gijp, K.L. Vincken, Medical students' cognitive load in volumetric image interpretation: insights from human-computer interaction and eye movements, Comput. Hum. Behav. 62 (September) (2016) 394–403.
[76] R. Rettie, An exploration of flow during Internet use, Internet Research: Electronic Networking Applications and Policy 11 (2) (2001) 103–113.
[77] D. Lee, J.Y. Chung, H. Kim, Text me when it becomes dangerous: exploring the determinants of college students' adoption of mobile-based text alerts short message service, Comput. Hum. Behav. 29 (3) (2013) 563–569.
[78] R.E. Petty, D.T. Wegener, Attitude change: multiple roles for persuasion variables, The Handbook of Social Psychology, McGraw-Hill, New York, NY, 1998, pp. 323–390.
[79] M. Dehghani, M.K. Niaki, I. Ramezani, R. Sali, Evaluating the influence of YouTube advertising for attraction of young customers, Comput. Hum. Behav. 59 (June) (2016) 165–172.
[80] J.R. Zuwerink, P.G. Devine, Attitude importance and resistance to persuasion: it's not just the thought that counts, J. Pers. Soc. Psychol. 70 (5) (1996) 931–944.
[81] E. Hudlicka, To feel or not to feel: the role of affect in human–computer interaction, Int. J. Hum. Stud. 59 (1–2) (2003) 1–32.
[82] F. Belanger, J.S. Hiller, W.J. Smith, Trustworthiness in electronic commerce: the role of privacy, security, and site attributes, J. Strateg. Inf. Syst. 11 (3) (2002) 245–270.
[83] T. Cheng, D.Y. Lam, A.C. Yeung, Adoption of internet banking: an empirical study in Hong Kong, Decis. Support Syst. 42 (3) (2006) 1558–1572.
[84] B. Suh, I. Han, The impact of customer trust and perception of security control on the acceptance of electronic commerce, Int. J. Electron. Commer. 7 (3) (2003) 135–161.
[85] W.D. Salisbury, R.A. Pearson, A.W. Pearson, D.W. Miller, Perceived security and World Wide Web purchase intention, Ind. Manag. Data Syst. 101 (4) (2001) 165–177.
[86] D.-H. Shin, The effects of trust, security and privacy in social networking: a security-based approach to understand the pattern of adoption, Interact. Comput. 22 (5) (2010) 428–438.
[87] P. Luarn, H.-H. Lin, Toward an understanding of the behavioral intention to use mobile banking, Comput. Hum. Behav. 21 (6) (2005) 873–891.
[88] Y.S. Wang, H.H. Lin, P. Luarn, Predicting consumer intention to use mobile service, Inf. Syst. J. 16 (2) (2006) 157–179.
[89] I. Arpaci, Understanding and predicting students' intention to use mobile cloud storage services, Comput. Hum. Behav. 58 (2016) 150–157.
[90] P.B. Lowry, J. Gaskin, G.D. Moody, Proposing the multimotive information systems continuance model (MISC) to better explain end-user system evaluations and continuance intentions, J. Assoc. Inf. Syst. 16 (7) (2015) 515–579.
[91] D. Liu, X. Li, R. Santhanam, Digital games and beyond: what happens when players compete, MIS Q. 37 (1) (2013) 111–124.
[92] P.B. Lowry, J. Gaskin, N.W. Twyman, B. Hammer, T.L. Roberts, Taking "fun and games" seriously: proposing the hedonic-motivation system adoption model (HMSAM), J. Assoc. Inf. Syst. 14 (11) (2013) 617–671.
[93] G.-H. Huang, N. Korfiatis, Trying before buying: the moderating role of online reviews in trial attitude formation toward mobile applications, Int. J. Electron. Commer. 19 (4) (2015) 77–111.
[94] D. Fonseca, N. Martí, E. Redondo, I. Navarro, A. Sánchez, Relationship between student profile, tool use, participation, and academic performance with the use of Augmented Reality technology for visualized architecture models, Comput. Hum. Behav. 31 (February) (2014) 434–445.
[95] J.L. Jenkins, B.B. Anderson, A. Vance, C.B. Kirwan, D. Eargle, More harm than good? How messages that interrupt can make us vulnerable, Inf. Syst. Res. 27 (4) (2016) 880–896.
[96] S.A. Nasco, S. Kulviwat, A. Kumar, I. Bruner, C. Gordon, The CAT model: extensions and moderators of dominance in technology acceptance, Psychol. Mark. 25 (10) (2008) 987–1005.
[97] J.S. Valacich, D.V. Parboteeah, J.D. Wells, The online consumer's hierarchy of needs, Commun. ACM 50 (9) (2007) 84–90.
[98] K.J. Kim, S.S. Sundar, Does screen size matter for smartphones? Utilitarian and hedonic effects of screen size on smartphone adoption, Cyberpsychol. Behav. Soc. Netw. 17 (7) (2014) 466–473.
[99] A. Burton-Jones, D.W. Straub Jr, Reconceptualizing system usage: an approach and empirical test, Inf. Syst. Res. 17 (3) (2006) 228–246.
[100] D. Gefen, E. Karahanna, D.W. Straub, Inexperience and experience with online stores: the importance of TAM and trust, IEEE Trans. Eng. Manag. 50 (3) (2003) 307–321.
[101] D. Gefen, E. Karahanna, D.W. Straub, Trust and TAM in online shopping: an integrated model, MIS Q. 27 (1) (2003) 51–90.
[102] P.B. Lowry, G. Moody, A. Vance, M. Jensen, J. Jenkins, T. Wells, Using an elaboration likelihood approach to better understand the persuasiveness of website privacy assurance cues for online consumers, J. Assoc. Inf. Sci. Technol. 63 (4) (2012) 755–776.
[103] A. Vance, C. Elie-Dit-Cosaque, D.W. Straub, Examining trust in information technology artifacts: the effects of system quality and culture, J. Manag. Inf. Syst. 24 (4) (2008) 73–100.
[104] S. Boss, D. Galletta, P.B. Lowry, G.D. Moody, P. Polak, What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors, MIS Q. 39 (4) (2015) 837–864.
[105] A.J. Burns, T.L. Roberts, C. Posey, P.B. Lowry, Examining the influence of organizational insiders' psychological capital on information security threat and coping appraisals, Comput. Hum. Behav. 68 (March) (2017) 190–209.
[106] A.C. Johnston, M. Warkentin, Fear appeals and information security behaviors: an empirical study, MIS Q. 34 (3) (2010) 549–566.
[107] P. Menard, M. Warkentin, P.B. Lowry, The impact of collectivism and psychological ownership on protection motivation: a cross-cultural examination, Comput. Secur. 75 (June) (2018) 147–166.
[108] C. Posey, T.L. Roberts, P.B. Lowry, The impact of organizational commitment on insiders' motivation to protect organizational information assets, J. Manag. Inf. Syst. 32 (4) (2015) 179–214.
[109] M.-H. Huang, Designing website attributes to induce experiential encounters, Comput. Hum. Behav. 19 (4) (2003) 425–442.
[110] C.L. Hollingsworth, A.B. Randolph, Using NeuroIS to better understand activities performed on mobile devices, Information Systems and Neuroscience, Springer, 2015, pp. 213–219.
[111] K.B. Murray, S. Bellman, Productive play time: the effect of practice on consumer demand for hedonic experiences, J. Acad. Mark. Sci. 39 (3) (2011) 376–391.
[112] C. Li, R. Meeds, Different forced-exposure levels of internet advertising: an experimental study on pop-up ads and interstitials, Paper Presented at the Proceedings of the 2005 Conference of the American Academy of Advertising, East Lansing, MI, 2005, pp. 200–207.
[113] H. Li, S.M. Edwards, J.-H. Lee, Measuring the intrusiveness of advertisements: scale development and validation, J. Advert. 31 (2) (2002) 37–47.
[114] F. Rejón-Guardia, F.J. Martínez-López, Online advertising intrusiveness and consumers' avoidance behaviors, in: F.J. Martínez-López (Ed.), Handbook of Strategic e-Business Management, Springer, Berlin, Heidelberg, 2014, pp. 565–586 Berlin Heidelberg.
[115] L. Ying, T. Korneliussen, K. Grønhaug, The effect of ad value, ad placement and ad execution on the perceived intrusiveness of web advertisements, Int. J. Advert. 28 (4) (2009) 623–638.
[116] S.M. Edwards, H. Li, J.-H. Lee, Forced exposure and psychological reactance: antecedents and consequences of the perceived intrusiveness of pop-up ads, J. Advert. 31 (3) (2002) 83–95.
[117] V. Venkatesh, M.G. Morris, B.D. Gordon, F.D. Davis, User acceptance of information technology: toward a unified view, MIS Q. 27 (3) (2003) 425–478.
[118] C.L. Anderson, R. Agarwal, Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions, MIS Q. 34 (3) (2010) 613–643.
[119] D. Yin, S.D. Bond, H.A.N. Zhang, Keep your cool or let it out: nonlinear effects of expressed arousal on perceptions of consumer reviews, J. Mark. Res. 54 (3) (2017) 447–463.
[120] R.A. Siddiqui, A. Monga, E.C. Buechel, When intertemporal rewards are hedonic, larger units of wait time boost patience, J. Consum. Psychol. 28 (4) (2018) 612–628.
[121] C.M. Angst, R. Agarwal, Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion, MIS Q. 33 (2) (2009) 339–370.
[122] H.W. Marsh, D. Hocevar, Application of confirmatory factor analysis to the study of self-concept: first- and higher order factor models and their invariance across groups, Psychol. Bull. 97 (3) (1985) 562–582.
[123] J.F. Hair, R.L. Tatham, R.E. Anderson, W. Black, Multivariate Data Analysis Vol. 6 Pearson Prentice Hall, Upper Saddle River, NJ, 2006.
[124] P.M. Podsakoff, S.B. MacKenzie, N.P. Podsakoff, Sources of method bias in social science research and recommendations on how to control it, Annu. Rev. Psychol. 63 (January) (2012) 539–569.
[125] W.W. Chin, Frequently Asked Questions – Partial Least Squares & PLS-Graph, from (2000) http://disc-nt.cba.uh.edu/chin/plsfaq.htm.
[126] A.J. Burns, T.L. Roberts, C. Posey, P.B. Lowry, The adaptive roles of positive and negative emotions in organizational insiders' engagement in security-based precaution taking, Inf. Syst. Res. 2019 (2019) forthcoming.
[127] 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.

Dr. Dezhi Wu (dezhiwu@cec.sc.edu) is an associate professor in the Department of Integrated Information Technology, University of South Carolina, Columbia, SC, USA. She explores how users interact with computers, the Internet, robotics and smart devices, as well as other emerging technologies, to accomplish their goals. Her passion also extends to creating innovative and cutting-edge interfaces and designing transformative experiences that fill the gaps between users and today's evolving technologies. Her research has been widely published in the *Computers in Human Behavior*, *Information & Management*, *Communications of the Association for Information Systems*, *Journal of Information Systems Security*, *Computers & Education*, *IEEE Internet Computing*, and others in addition to ICIS, HICSS, AMCIS, PACIS and HCII conference proceedings. She served as the Chair for AIS SIGHCI (http://sighci.org/) and is currently serving as an advisory board member for the SIGHCI. She regularly chairs the HCI tracks and workshops for several leading conferences including ICIS, AMCIS, PACIS and HCII. She is currently serving as an associate editor for *AIS Transactions on Human-Computer Interaction*, and an associate editor for a gamification special issue for *European Journal of Information Systems*.

Dr. Gregory D. Moody (greg.moody@unlv.edu) is currently the Lee Professor of Information Systems in the Management, Entrepreneurship and Technology Department in the Lee Business School at the University of Nevada, Las Vegas and Director of the Graduate MIS program. Her received a Ph.D. from the University of Pittsburgh and a Ph.D. from the University of Oulu. He has published in *MIS Quarterly, Information Systems Research, Journal of Management Information Systems, JAIS, EJIS, ISJ*, and other journals. His interests include IS security and privacy, e-business (electronic markets, trust) and human–computer interaction (Web site browsing, entertainment). He is currently a senior editor for ISJ and the AIS Transactions on Human-Computer Interaction (THCI), the previous president of Special Interest Group on Human-Computer Interaction (SIGHCI), and the Managing Editor for THCI.

Dr. Jun Zhang (jzhang90@ustc.edu.cn) is currently an assistant professor in MIS at the International Institute of Finance, School of Management, University of Science and Technology of China. He holds a Ph.D. in information systems from City University of Hong Kong. His research centers on online deviant behaviors, information privacy and security, and IT-enabled health behavior change. His research has been published in journals such as *Information Systems Research, Journal of Management Information Systems,* and *Computers in Human Behavior*. He has served as a guest associate editor at the EJIS, as well as an associate editor at ICIS 2018 and ECIS 2020.

Professor Paul Benjamin Lowry (paul.lowry.phd@gmail.com) is the Suzanne Parker Thornhill Chair Professor and Eminent Scholar in Business Information Technology at the Pamplin College of Business at Virginia Tech. He is also the BIT Ph.D. program director. He is a former tenured Full Professor at the City University of Hong Kong and The University of Hong Kong. He received his Ph.D. in Management Information Systems from the University of Arizona and an MBA from the Marriott School of Management. He has published 125+ journal articles in *MIS Quarterly, Information Systems Research, Journal of Management Information Systems, J. of the AIS, Information System J., European J. of Information System, J. of Strategic IS, J. of IT, Decision Sciences J., Information & Management,* and others. He is a department editor at *Decision Sciences J*. He also is an SE at *JMIS, JAIS*, and *ISJ*, and an AE at the *EJIS*. He has also served multiple times as track co-chair at ICIS, ECIS, and PACIS. His research interests include (1) organizational and behavioral security and privacy; (2) online deviance, online harassment, and computer ethics; (3) HCI, social media, and gamification; and (4) business analytics, decision sciences, innovation, and supply chains.