Information Systems Research

Publication details, including instructions for authors and subscription information:
http://pubsonline.informs.org

Examining the Continuance of Secure Behavior: A Longitudinal Field Study of Mobile Device Authentication

Paul John Steinbart, Mark J. Keith, Jeffry Babb

To cite this article:
Paul John Steinbart, Mark J. Keith, Jeffry Babb (2016) Examining the Continuance of Secure Behavior: A Longitudinal Field Study of Mobile Device Authentication. Information Systems Research 27(2):219-239. https://doi.org/10.1287/isre.2016.0634

Information Systems Research
Vol. 27, No. 2, June 2016, pp. 219–239
ISSN 1047-7047 (print) | ISSN 1526-5536 (online)

http://dx.doi.org/10.1287/isre.2016.0634

Examining the Continuance of Secure Behavior: A Longitudinal Field Study of Mobile Device Authentication

Paul John Steinbart
Department of Information Systems, Arizona State University, Tempe, Arizona 85287, paul.steinbart@asu.edu

Mark J. Keith
Information Systems Department, Brigham Young University, Provo, Utah 84602, mark.keith@gmail.com

Jeffry Babb
Department of Computer Information Systems and Decision Management, West Texas A&M University, Canyon, Texas 79016, jbabb@wtamu.edu

It is not enough to get information technology (IT) users to adopt a secure behavior. They must also *continue* to behave securely. Positive outcomes of secure behavior may encourage the continuance of that behavior, whereas negative outcomes may lead users to adopt less-secure behaviors. For example, in the context of authentication, login success rates may determine whether users continue to use a strong credential or switch to less secure behaviors (e.g., storing a credential or changing to a weaker, albeit easier to successfully enter, credential). Authentication is a particularly interesting security behavior for information systems researchers to study because it is affected by an IT artifact (the design of the user interface). Laptops and desktop computers use full-size physical keyboards. However, users are increasingly adopting mobile devices, which provide either miniature physical keypads or touchscreens for entering authentication credentials. The difference in interface design affects the ease of correctly entering authentication credentials. Thus, the move to use of mobile devices to access systems provides an opportunity to study the effects of the user interface on authentication behaviors. We extend existing process models of secure behaviors to explain what influences their (dis)continuance. We conduct a longitudinal field experiment to test our predictions and find that the user interface does affect login success rates. In turn, poor performance (login failures) leads to discontinuance of a secure behavior and the adoption of less-secure behaviors. In summary, we find that a process model reveals important insights about how the IT artifact leads people to (dis)continue secure behaviors.

Keywords: continuance of security behavior; security behaviors; authentication; password; passphrase; mobile computing; smartphone; usability; user interface; longitudinal research; field experiment
History: Radhika Santhanam, Senior Editor; Alessandro Acquisti, Associate Editor. This paper was received on March 19, 2014, and was with the authors 8 months for 3 revisions. Published online in *Articles in Advance* May 19, 2016.

1. Introduction

Although a large and growing body of research (Anderson and Agarwal 2010, Dinev and Hu 2007, Huang et al. 2011, Lee and Larsen 2009, Liang and Xue 2010) has shed light on the factors that influence a user's *initial* adoption of secure behaviors, there has been little research about the long-term *continuance* of secure behaviors. This gap is important because persuading people to adopt a desirable security practice is of limited value if they subsequently discontinue it and revert to less-secure behaviors. Research has shown that initial use decisions are different from decisions to continue using that system (Agarwal and Karahanna 2000, Bhattacherjee 2001, Karahanna et al. 1999, Kim et al. 2007, Taylor and Todd 1995, Venkatesh and Bala 2008). In particular, actual experience using a system moderates the influence of intentions and attitudes on subsequent behavior (Hong et al. 2008; Limayem et al. 2007; Venkatesh et al. 2008, 2012). For example, people tend to disable or stop using security features that are inconvenient or difficult to perform (Adams and Sasse 1999).

Authentication controls are a critical part of an information security program because their objective is to limit system access to only authorized individuals. Three types of authentication credentials are commonly used: something you know (e.g., a PIN, password, or passphrase), something you have (e.g., a smart card or USB token), or something you are (e.g., biometric identifiers such as fingerprints, voice recognition, etc.). Of these three types of credentials,

the first is ubiquitous. Indeed, in many systems, a user name and a password (or equivalent) is the only authentication credential used. Even when systems require multiple credentials, a practice referred to as multifactor authentication, passwords usually are one of those factors. Thus, password usability remains an important security topic.

A well-documented challenge in the use of password-based authentication is the trade-off between security and ease of use (Brown et al. 2004; Huang et al. 2011; Ives et al. 2004; Keith et al. 2007, 2009; Yan et al. 2004; Zviran and Haga 1999). For example, people tend to create passwords that are easy to remember, which often means that they are also easy to guess. The importance of ease of use means that features of the information technology (IT) artifact, such as the nature of the user interface (UI), are likely to be key determinants of the decision to continue a secure authentication behavior.

The potential effect of the design and implementation of the UI on secure authentication behavior is particularly relevant in light of the ever-increasing use of mobile devices (e.g., phones, tablets, etc.) to access and store sensitive information in financial systems and social networks. Whereas desktop and laptop computers provide full-size physical keyboards for entering authentication credentials, mobile devices possess miniature keyboards or, increasingly, touchscreens, which represent flat facsimiles of a traditional keyboard. These differences in the UI make data entry both slower and more error prone when using mobile devices rather than desktop or laptop computers (Bao et al. 2011, Jakobsson and Akavipat 2012, Lee and Zhai 2009, Park et al. 2008).

Consequently, if people experience difficulty in entering strong authentication on mobile devices, they may be tempted to discontinue a secure authentication behavior (e.g., the use of a strong authentication credential) and adopt a less-secure, but easier to successfully perform, alternative. For example, they may store the password on their device and configure it to automatically submit it whenever accessing a remote system. Such behavior seriously weakens authentication security—particularly in light of the millions of reported incidents of mobile device loss or theft each year (ConsumerReports 2014). People also sometimes "loan" their phone to others (Ben-Asher et al. 2011, Karlson et al. 2009). Whether lost, stolen, or loaned, the result is that an unauthorized person has physical possession of the device. Therefore, if the device was configured to automatically submit authentication credentials, the risk of unauthorized access to systems that contain sensitive information is high.

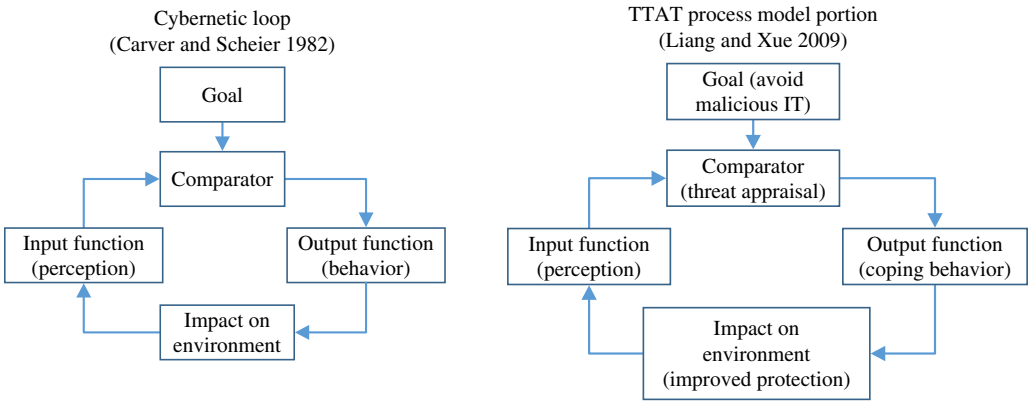
This study makes several important contributions to the security literature. First, we examine the factors that influence the *continuation* of secure behaviors. We use the results of psychology research on memory structures and the modification of decision strategies to extend existing information systems (IS) process models of security behavior (Liang and Xue 2009). Specifically, we characterize individuals' attempts to behave securely as part of a cybernetic loop that influences subsequent behavior (Carver and Scheier 1982, Wiener 1948). Our second contribution is methodological. Two of the greatest difficulties in information privacy and security research are (1) collecting valid measures of real user behaviors and (2) monitoring these behaviors over time (Belanger and Crossler 2011, Smith et al. 2011). We address those problems by designing a longitudinal field experiment that allows us to observe people's authentication behaviors in a natural setting, rather than in a controlled laboratory experiment. This increases the likelihood that the behaviors we observe are representative of those likely to occur in practice. In particular, we investigate how the UI, specifically the means (touchscreen versus full-size physical keyboard) used to enter authentication credentials to obtain access to a remote system, affects continuance of authentication behaviors. Our results suggest that despite mechanisms designed to improve the usability of mobile keyboards (e.g., displaying the last character typed), mobile interfaces clearly hinder the continuance of secure authentication behaviors. Consequently, the mobile interface may be the catalyst that finally shifts—indeed, is currently shifting—the security paradigm away from relying primarily (and in many cases, solely) on text-entry-based authentication and toward the use of multifactor approaches that include other types of credentials (e.g., biometrics).

2. Literature Review and Theory

Voluntary security behaviors in nonworkplace settings have received increased research attention over the past decade. For example, studies have examined the use of antimalware to protect computers (Dinev and Hu 2007, Johnston and Warkentin 2010, Lee and Larsen 2009, Liang and Xue 2010), the use of firewalls to control access to home wireless networks (Woon et al. 2005), and intent to engage in protective behaviors to respond to computer security threats in general (Anderson and Agarwal 2010).

This stream of research has primarily drawn on protection motivation theory (Rogers 1975, Tanner et al. 1991) to explain how and why people choose to behave securely. Liang and Xue (2009) developed an IS-specific variant, which they called Technology Threat Avoidance Theory (TTAT), designed to specifically focus on computer security. According to TTAT, secure behaviors represent a coping response to recognized threats. The two most important antecedents

Figure 1 (Color online) Cybernetic Loop and TTAT Process Model



Source. Adapted from Liang and Xue (2009).

of secure behaviors are (1) perceptions that a threat is serious (i.e., has a high likelihood of occurring and results in severe consequences) and (2) perceptions that the threat is avoidable because there exist effective countermeasures that can be performed without excessive cost or effort.

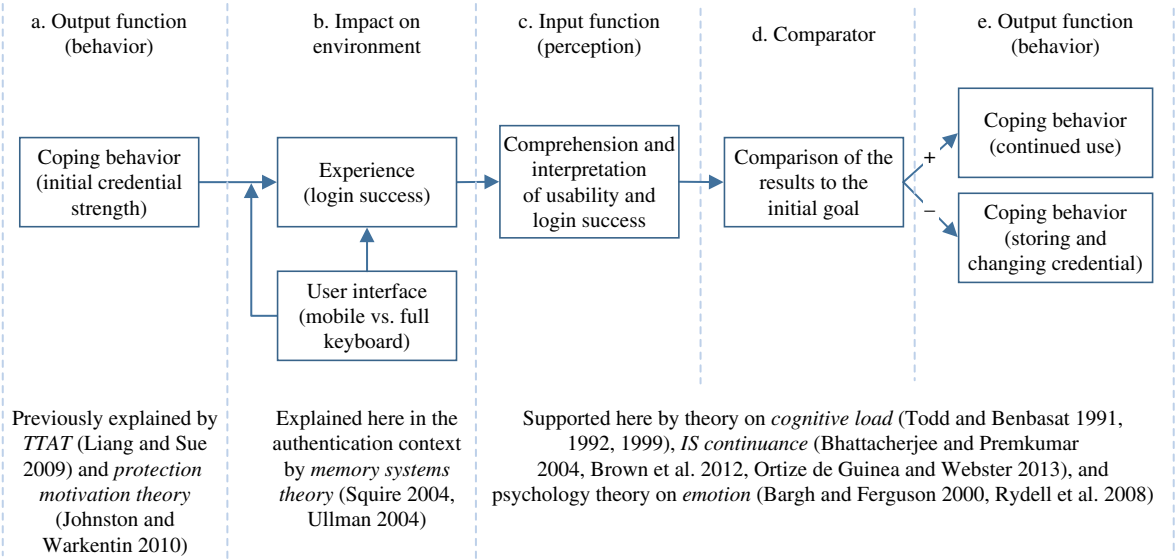
This variance model has been validated in a number of studies (e.g., Johnston and Warkentin 2010, Liang and Xue 2010). However, TTAT also includes a process model explaining the continuance of security behaviors that has received significantly less attention from researchers. The process model is based on a cybernetic feedback loop (Carver and Scheier 1982). One of the core concepts of cybernetic theory (Wiener 1948) is that human beings constantly adjust their behavior toward an end goal via cybernetic feedback loops (Carver and Scheier 1982). A cybernetic loop consists of a goal, comparator, input function, environmental impacts, and output function (see Figure 1).

The cybernetic loop begins when there is a disturbance to either the environment (e.g., the user's password is cracked) or the goal (e.g., IT manager dictates a stronger password). Consider, for example, that someone has purchased a new mobile device and would like to use it for financial transactions such as online banking or investments. However, the financial institution likely has a security policy that requires use of an authentication credential that meets certain guidelines. Or, the user voluntarily chooses to create a strong authentication credential. Either way, the result is a new *goal*: to create and use a strong credential to access the remote system. The user *compares* their present state (weak or no authentication credential) to their desired state (strong credential). The result of that comparison triggers the *output function*. The output function represents the behavior intended to eliminate the discrepancy—in this case, the creation of a stronger password. The *impact on the environment* is that the user's credential is now more resistant to password guessing and cracking. If the credential is not sufficiently strong, the *input function* senses the noncompliance, compares it to a reference point (*comparator*), which may be either an internal standard or an explicit requirement embedded in the remote system, and the loop repeats until the goal is achieved. Thus, the task of creating a strong credential can be explained as an iterative process in which the user continually refines the credential until it becomes satisfactory based on system feedback.

However, if there is a disturbance in the environment, the cybernetic loop may continue even *after* a credential is created. After creating a strong credential, another important factor emerges—the ease of remembering and typing that credential to authenticate to the system. Strong credentials may satisfy the goal of providing more security, yet be difficult to use (Brown et al. 2004; Keith et al. 2007, 2009). If a strong authentication credential results in more failed login attempts, a new goal surfaces: to make the credential more usable. The output function represents the behavior(s) designed to achieve this new goal, including (1) becoming skilled at remembering and typing the credential correctly, (2) changing the credential to something that is still compliant with policy, but easier to use, or (3) storing the credential so that it does not have to be continuously reentered. The latter two coping mechanisms may weaken security. Figure 2 depicts the cybernetic loop of TTAT in a sequential (rather than looped) model (as depicted in Figure 1) beginning with an initial output function behavior and including a subsequent output function.

In summary, following the example of TTAT, we adopt the cybernetic feedback loop (Carver and Scheier 1982, Liang and Xue 2009, Wiener 1948) as our core theory to explain the continuance of secure authentication behaviors. We extend that basic model by using relevant reference disciplines to explain steps B through E in Figure 2 in more detail. In

Figure 2 (Color online) Two Cycles Through the Cybernetic Feedback Loop



particular, we draw on research on memory systems (Ullman 2004) to explain how the user interface influences (dis)continuance of a secure authentication behavior (step B of Figure 2). We draw from theory on IS continuance and psychology theory concerning the influence of perceived effort and emotions on decision strategies to explain how user perceptions and reactions to performing the security behavior (step C of Figure 2) influence the decision to either continue to engage in that behavior or to switch to an alternative designed to bring the user's existing state and goal state in line (steps D and E of Figure 2).

2.1. Environmental Impacts: Memory Systems and the User Interface

Many security behaviors require both recall of knowledge and skill in applying that knowledge. For example, successful authentication to a system requires both remembering the credential linked to that system and then correctly entering it. Similarly, encrypting sensitive information requires recognizing the need to encrypt something and knowing how to do so. Sometimes the objective is to learn what not to do (e.g., reduce the risk of malware by not clicking on URL links embedded in email) and then practicing such restraint. Research on memory structure, particularly the distinction between *declarative* and *procedural* memory (Squire 1986), provides an explanation of how these two components of security behavior tasks (recall and procedures) jointly interact to affect task success.

2.1.1. Role of Human Memory Systems. Authentication credentials should be easy to remember and use yet also be resistant to guessing and brute-force enumeration attacks. The nature of human memory makes it difficult to satisfy both objectives. New information (e.g., authentication credentials) is initially stored in short-term memory until it can be transferred to long-term memory (Ullman 2004). This process is aided by rehearsal and "chunking" the information held in short-term memory (Baddeley 1994). Chunking refers to the ability to group information together (e.g., letters into words, words into phrases) to aid retention. Meaningful information is easier to remember (Ebbinghaus 1913). Words with speech sounds similar to previously learned words are also easier to store (see the *phonological similarity effect*; Baddeley 2012), which explains why mnemonic passwords are easier to remember than random ones (Yan et al. 2004). This phenomenon also likely accounts for the widespread use of common words and personal information as passwords (Johansson and Riley 2005). However, "simple" authentication credentials comprised of common words found in dictionaries, such as *fluffy* or *nonetheless*, are weak because they are easily guessed or cracked through brute-force enumeration techniques. Credentials that add one or more numbers either before or after a common word, such as *579rhyme* or *ready123*, or that replace letters with symbols, such as *p@$$w0rd*, are also "simple" because they, too, are weak and easily cracked. Therefore, most organizations have password policies that prohibit the use of common words as part of an authentication credential and instead require users to create credentials that include a mix of uppercase and lowercase letters, numbers, and special characters. Credentials that satisfy those constraints, such as *Tq7#P@m9*, are considered "complex" and are stronger and more resistant to attack. However, such complex credentials are also quite unlike

existing words and phrases already stored in memory. Novel words and phrases are more difficult to store and recall (Squire 2004). Thus, we would expect that it should be harder to remember complex than simple passwords.

However, it is also possible to use a pass*phrase* as a credential. Because a credential's resistance to brute-force attacks is affected more by its length than by the size of the character set, there are arguments that long passphrases consisting solely of uppercase and lowercase letters are stronger than shorter passwords that include nonletter characters (Keith et al. 2007, 2009). Moreover, because the entire phrase (e.g., *IwentsnorkelingintheNationalParkatKeyBiscayne*) is used, rather than using only specific characters from the phrase (e.g., using the first letter of each word in the preceding phrase to create *IwsitNPaKB*) to create a shorter password, it should be easier to correctly recall passphrases than complex passwords. Indeed, evidence indicates that passphrases result in fewer memory-based errors in recall (Jakobsson and Akavipat 2012) and fewer actual login failures based on memory failures (Keith et al. 2007, 2009) than passwords. By contrast, passwords comprised of 12 characters that do not constitute a meaningful phrase are hard to remember (Paul et al. 2011).

Thus far, we have discussed the process of creating and initially learning a new authentication credential. However, to retain knowledge, it must be transferred from short-term into long-term memory (Baddeley 2012). Long-term memory can be divided into two primary types: declarative and procedural. The declarative memory system underlies the learning and retention of facts and events (Ullman 2004)—it is the type referred to as "memory" in everyday language (Squire 2004). Declarative memory is almost entirely explicit, meaning it is available at a conscious level. Although authentication credentials may be initially stored as *episodic* declarative memory—meaning they are tied closely to the cues and details relevant to the event of creating it—they are eventually stored as facts, making them *semantic* declarative memories. Whereas episodic memories are very event specific and context specific—making them less transferrable from one situational recall to another—semantic memories are relatively easier to recall across contexts (e.g., entering the same password on multiple computers).

The preceding discussion explains how declarative memory affects credential recall. However, authentication credentials must not only be *recalled* correctly but also *entered* correctly into a login prompt. This is the role of procedural memory (Ullman 2013). The procedural memory system represents the motor skills learned from performing a given action or sequence of actions and rules repeatedly (Squire 2004). Procedural memory represents our nonconscious implicit motor skills such as riding a bicycle or entering a password or passphrase via a physical keyboard or touch screen.

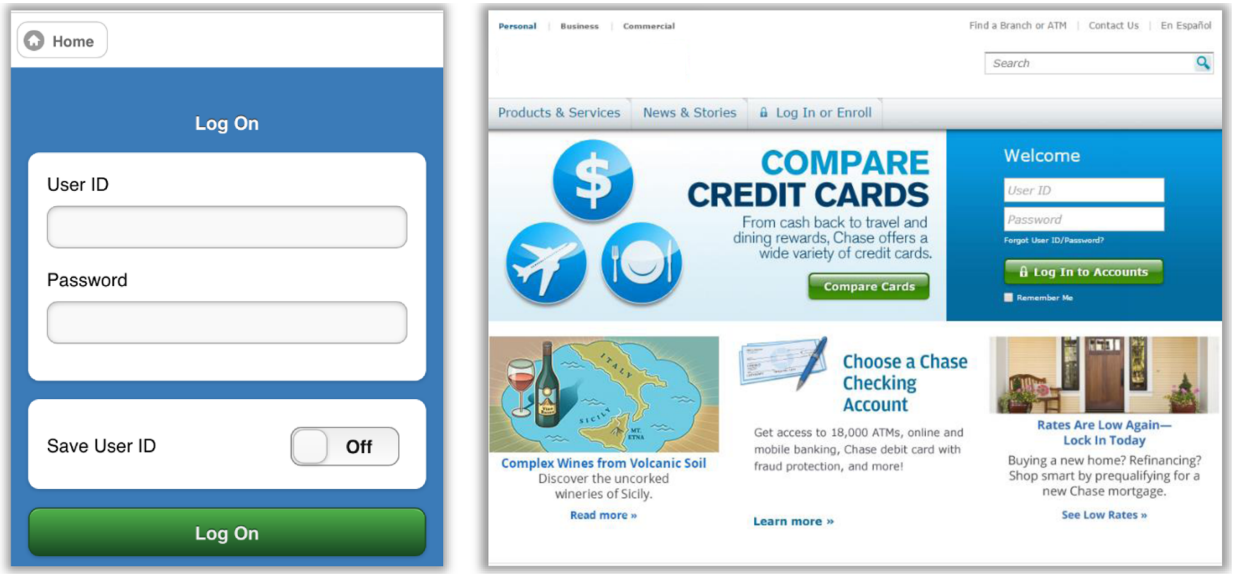
In summary, authentication credentials are learned in a process that begins with short-term memory, where the credential is rehearsed long enough to transfer it to long-term memory. During initial use of the credential, the user relies primarily on declarative memory to recall it. Then, with practice in entering the credential, it becomes stored in procedural memory. Eventually, because declarative memory tends to decay quickly (Ullman 2004), a user may rely primarily on procedural memory to correctly enter the credential. Credentials that are either adequately rehearsed, well "chunked," based on meaningful information, or comprised of known words and phrases (or some combination of those factors) will be more easily stored in short-term memory and transferred to declarative memory. Thus, simple passwords and passphrases should be easier to learn and recall than complex passwords comprised of randomly scrambled different types of characters. Furthermore, because complex credentials violate normal typing rules they are more difficult to learn how to enter correctly and, therefore, to store in procedural memory than are either simple passwords or "word-processing-compatible" passphrases (i.e., those that use natural words, follow normal rules for capitalization and punctuation, and incorporate numbers as part of dates). Difficulty in retrieving the credential from declarative memory increases the likelihood of login failures due to memory problems; poor procedural memory increases the likelihood of login failures due to typographical errors. Thus, the preceding discussion leads to our first hypothesis:

Hypothesis 1 (H1). *Authentication credential complexity is positively related to login failures.*

2.1.2. Effect of the User Interface. The authentication task environment, including the UI[1] of any IT artifacts employed, may affect both recall of information from declarative memory and the use of procedural knowledge. The UI can affect recall of information from declarative memory by altering the salience of cues. Cues that facilitate recall can be verbal, written, or graphical (Tulving and Pearlstone 1966). In particular, images and text that are present when new information is stored in working memory and transferred

[1] It should be noted that there are many elements of the UI including graphical design of the form, text boxes, buttons, lists, data input controls, etc. (Shneiderman 1986). The elements most relevant to the authentication context include the layout of the keyboard (i.e., where the buttons reside), the total number of key presses required to enter a credential, the properties of the password input box, and the graphical- and text-based cues included on the authentication form screen.

Figure 3 **(Color online) Example of Graphical- and Text-Based Cue Differences for Desktop and Mobile Interfaces**



to long-term memory are effective cues that aid in retrieving that information from long-term memory at a later time (Ericsson and Kintsch 1995). For example, the images incorporated into advertising campaigns are remarkably effective at helping consumers recall brand names (Keller 1987).

To understand the role of retrieval cues in credential recall, consider the recommendation to use a different password for each information system (Ives et al. 2004). Since different passwords are used across systems, the text and graphical content of the UI serves as a cue to help a person recall the correct password. Consequently, changing the UI, for example, by switching from a desktop to mobile (MacKay et al. 2004, Wiedenbeck et al. 2005), changes a website's content and, therefore, may disrupt declarative recall, thereby increasing login failures. As an example, Figure 3 depicts both the desktop and mobile versions of the login screen for JPMorgan Chase. The desktop version contains a variety of images and text that are not present in the mobile version. Indeed, the textboxes and button that allow authentication comprise only a portion of the desktop screen, whereas the mobile version is entirely occupied by the authentication interface. As a result, the user cannot use any of the desktop cues to aid recall on the mobile UI.

The nature of the UI can also affect the ability to use procedural knowledge. Full-size physical keyboards clearly display all possible characters and require at most the use of two keys simultaneously to capitalize a letter or enter a special character. By contrast, most touchscreens on mobile devices require considerable effort to change between lowercase and uppercase letters, or to select numbers and special characters. For example, Jakobsson and Akavipat (2012) point out that it takes 21 actions to enter the 12-character credential "*flY2theM0On!*" on a touchscreen, but requires only 15 key presses if using a physical keyboard. It also requires interrupting the data entry process to decide whether a particular character is on the current screen (Sears and Zha 2003). Consequently, typing on touchscreens is inherently more error prone than typing on keyboards (Lee and Zhai 2009, Park et al. 2008). Indeed, studies have found that it takes two to three times longer to enter a typical complex password on a mobile device with a touchscreen or miniature keyboard than when entering the same credential via a full-sized physical keyboard (Bao et al. 2011). As a result, the touchscreen UI is clearly a unique context from traditional keyboards. As discussed above, procedural memory is difficult to transfer from one context to another (Ullman 2013).

Thus, the UI can affect login success by making it harder to both (1) recognize the cues used to recall the correct authentication credential from declarative memory and (2) by restricting the user's ability to draw from procedural memory. This leads to our second hypothesis:

Hypothesis 2 (H2). *Login failures will be greater when entering authentication credentials using a miniature keyboard or touchscreen than when using a normal-sized physical keyboard.*

In addition to directly affecting login success, there is reason to believe that the UI will also moderate the effect of strong credentials on login success. Because the declarative and procedural memory systems interact cooperatively in human learning and processing, negative effects in one system may lead to negative effects on the other (Ullman 2004, 2013). This interdependent relationship was identified specifically in

the context of a word recall experiment. After disrupting the procedural memory system, participants performed lower on a word recall task than the control group (Brown and Robertson 2007).

This interrelationship between the declarative and procedural memory systems suggests how the design of the UI can affect performance of a security task. Most people have developed procedural knowledge for typing their authentication credentials on the full-sized physical keyboards found on laptop and desktop computers, and can do so with a high rate of success. The different UI found on a mobile device, however, precludes drawing on that previously acquired procedural memory to enter a password with minimal conscious effort. Instead, users must consciously search for whether each character in their credential is visible on the screen or requires pressing a key to access a different touchscreen, while retaining the entire credential in memory. This heightened cognitive burden increases the difficulty of learning the new procedural knowledge (Keisler and Shadmehr 2010), thereby increasing the likelihood of login failures due to typing errors. If repeated, such failures may cause users to question whether they are recalling the correct information (i.e., authentication credential) for the task. As a result, the person may then try to resolve the problem by recalling and using different information. Thus, an initial error in applying procedural knowledge (e.g., unsuccessfully entering an authentication credential because of a typographical mistake) may cause a subsequent error in the declarative memory system (e.g., recalling the wrong credential).

Thus, the preceding discussion suggests that the difference between the UI provided on mobile devices and that found on laptops and desktop computers is likely to exacerbate the inherent difficulty of using strong passwords and leads to our third hypothesis:

Hypothesis 3 (H3). *The effect of credential strength on login failures will be greater when using a miniature keyboard or touchscreen than when using a normal-sized physical keyboard*.

2.2. The Comparator and the Outcome Function: How Experience Influences (Dis)Continuance

Based on the cybernetic feedback loop (Carver and Scheier 1982), after the environment has been disrupted (e.g., via switching to use of a mobile UI for authentication), the user must perceive this disruption (input function), and make a comparison between the new state and the desired state (comparator) that leads to new behavior (next output function) designed to bring the two states into congruence. In the context of authentication, the comparison between expectations and experience (step D in Figure 2) is binary: the user either successfully accesses the system or fails to do so. These two outcomes determine what happens in step E in Figure 2 (selection of a coping behavior).

According to cybernetic theory, success requires no change in behavior, because the user has obtained the desired goal. The desired state is what the user *expects*. Thus, when experience matches the desired state, it represents a confirmation of expectations. IS research on system use has shown that confirmation of expectations (and positive disconfirmation, i.e., finding that a system exceeds expectations) encourages continuance (Bhattacherjee and Premkumar 2004, Hong et al. 2006, Limayem et al. 2007). Hence, in the context of authentication, the login success should encourage continued use of the authentication credential.

By contrast, if the comparator (step D in Figure 2) evaluates current experience as not matching the desired state (e.g., in the context of authentication, a login failure), the user takes action (coping behavior, step E in Figure 2) to resolve the discrepancy. As shown in Figure 2, there are three possible responses to a failure to authenticate when using a particular credential. One is to keep using the same credential, repeating the process until achieving success via practice. Another alternative is to store the credential so that it is automatically submitted when authenticating. This solution eliminates login failures, regardless of whether caused by forgetting the credential or difficulty in correctly entering it. A third possible solution that also fixes both causes of login failures is to change to a different credential that is easier to remember and easier to type. The first alternative (continued use of a credential) is desirable because it maintains security at a given level, whereas the other two alternatives solve the problem, but do so at the expense of weakening security. Prior research in both IS and psychology suggests several reasons why people may discontinue using an authentication credential that results in login failures and switch to an alternative behavior instead.

Continued practice using an authentication credential will reduce login failures (Keith et al. 2007, 2009) while maintaining security, but requires time and effort. By contrast, the other possible alternatives (storing the credential for automatic submission or switching to a weaker credential that is easy to enter) *quickly* resolve the problem of login failures with minimal effort, but do so by weakening security. Research in psychology indicates that decision makers seek to maximize quality (accuracy) while simultaneously minimizing total effort (Payne 1982, Payne et al. 1993). IS research on decision aids has found that people's perceptions of required effort play a bigger role in their choice of which decision strategy to adopt than does consideration of the relative quality of those options (Todd and Benbasat 1991,

1992). In other words, people tend to trade off accuracy for effort. Moreover, this tendency persists even in the presence of explicit incentives related to accuracy (Todd and Benbasat 1999). This effort-accuracy trade-off may explain why people tend to discontinue performing security behaviors that are difficult to perform successfully (Adams and Sasse 1999). Therefore, it is reasonable to expect that people will respond to login failures when using a strong credential by discontinuing a difficult to perform behavior (manual entry of a strong authentication credential) and switching to an alternative behavior (e.g., storing their credential so that they do not have to manually enter it or switching to a weaker credential that is easier to enter) that requires less effort to perform successfully.

Whereas confirmation of expectations encourages continuance, negative disconfirmation of expectations (i.e., experiencing difficulties that were either unexpected or greater than anticipated) creates intentions to discontinue use (Bhattacherjee and Premkumar 2004, Brown et al. 2012, Ortiz de Guinea and Webster 2013). Moreover, those studies indicate that negative disconfirmation of expectations affects subsequent behavior both directly and, by creating dissatisfaction with the existing state of affairs, indirectly. The direct effect represents the role of cognitive perceptions on behavior, in that a discrepancy between the desired and actual states results in changing behavior to eliminate that discrepancy. The indirect effect, through dissatisfaction, represents the complementary role that emotions play on the decision to (dis)continuance (Ortiz de Guinea and Markus 2009).

Dissatisfaction is a negative emotion. There is evidence that "people are motivated to change or alter their environment when in negative moods and to leave well enough alone when in positive moods" (Bargh and Ferguson 2000, p. 932). Furthermore, negative emotions encourage risky behavior (Rydell et al. 2008). In the context of authentication, login failures are likely to be perceived negatively because they deny anticipated access. Therefore, the resulting dissatisfaction may encourage discontinuing the behavior (manual entry of a strong authentication credential) that causes the problem (login failure) and changing to behaviors (e.g., storing the credential for autosubmission or replacing it with a simpler one that is easier to enter) that solve the problem, but do so by increasing risk.

In summary, the preceding discussion suggests several complementary reasons why people are likely to respond to login failures (step E in the cybernetic loop depicted in Figure 2, coping behaviors) by discontinuing an existing authentication behavior and replacing it with a less secure behavior. Hence we offer the following multipart hypothesis:

Hypothesis 4A (H4A). *Login failures will increase the likelihood of storing an authentication credential and having it automatically submitted when attempting to access a remote system.*

Hypothesis 4B (H4B). *Login failures will increase the likelihood of changing an authentication credential to one that is easier to use* (*shorter or less complex*).

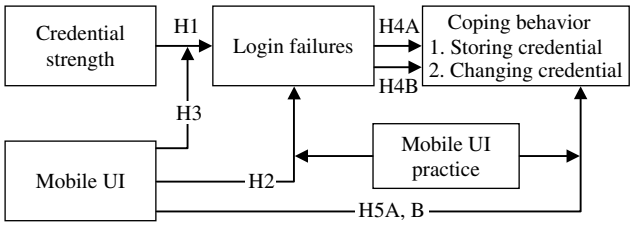
2.3. Effect of the User Interface on Coping Response

In addition to the effect of login failures, there is also reason to expect that the UI will directly influence authentication behaviors. As shown in Figure 2, the decision to (dis)continue a behavior is affected by comparing a person's experience in executing that behavior with the desired/expected state. When the desired and actual states match (i.e., when expectations are confirmed) people are likely to continue the behavior; but when those expectations are disconfirmed, they are likely to respond by discontinuing the behavior. The nature and design of the UI plays an important role on that process by affecting how easy (hard) it is to successfully execute a given behavior. Indeed, people's choice of a decision strategy can be influenced by changing the design of a decision aid so that it makes one strategy easier than another (Todd and Benbasat 1999). Moreover, ease of use should increase satisfaction and, thereby, the desire to continue using that system or performing a given behavior. By contrast, difficulties in use are likely to cause frustration and dissatisfaction, leading to discontinuance. In short, the UI can be either an enabler or inhibitor (Cenfetelli 2004) to the continuance of a security behavior.

As discussed earlier, the touchscreen interface provided on smartphones and other mobile devices makes it more difficult to enter long and complex authentication credentials, thereby increasing the likelihood of login failures due to typing errors. In addition, typing difficulties may also cause people to question whether they are entering the proper credential, which could, in turn, lead to login failures due to memory errors. Consequently, it is not surprising that many people report that they do not like using such an interface to enter authentication credentials (Trewin et al. 2012). Indeed, there is evidence that some people so dislike the process for entering passwords on touchscreens that they actively seek ways to avoid having to do so (Bao et al. 2011, Jakobsson and Akavipat 2012). This leads to the following multipart hypothesis:

Hypothesis 5A (H5A). *Ceteris paribus, users will be more likely to store their authentication credential when using a mobile UI.*

Figure 4 Theoretical Model and Hypotheses



Hypothesis 5B (H5B). *Ceteris paribus, users will be more likely to change their authentication credential to a simpler one when using a mobile UI.*

2.4. Effects of Practice and Learning

Through repeated practice, people develop procedural memory about how to perform a task (Ullman 2004). As a result, performance tends to improve over time. For example, Keith et al. (2007, 2009) found that over a three-month period, participants in their experiments experienced fewer login failures due to either typographical or memory errors when entering passphrases via full-size physical keyboards. Thus, it is reasonable to expect that any effects associated with using a mobile device to authenticate should decrease over time. Consequently, we explore whether practice using a mobile device to authenticate moderates the effects of the mobile device UI on login failures and coping behaviors. In summary, Figure 4 presents our research model hypotheses, and research questions.

3. Method

We created a mobile app with an accompanying website to conduct a field experiment to test the hypotheses. The mobile app was a game that allowed social interactions among players. This game required participants to login to the website frequently, using either personal computers (laptops or desktops) or a mobile device. The mobile app (called "findamine" or "find.a.mine" in the Apple App Store and Google Play) is a modified geo-caching game visualized in Figure 5.

Each week (for 12 weeks), three new clues were delivered to the participant's mobile device (either tablet or smartphone). They earned points by deciphering the clue and travelling to the location. If the participant was close enough (GPS-verified) to the location, they could click a "Found it!" button, which would prompt them to take a picture of themselves at the location through the mobile app. If the participant could not decipher the clue, the app provided a closeness meter (see Figure 5(d) and 5(e)) that indicated how geographically close they were to the target clue. This indicator updated in real time allowing the participant to find any clue as they travelled around. Participants earned game points for each clue found. Game points were summarized on the website leaderboard (see Figure 6). Participants had to authenticate through the website to view the leaderboard, photos of themselves and others, and details of each clue found (e.g., time span, location on a map, photo, points earned).

To encourage participants to return often to the game website (and attempt to authenticate), several other features were implemented. First, participants could create an online profile with a variety of personal and demographic information. Second, an online social network was incorporated into the game that allowed players to follow and track the progress of their friends, refer other players, and exchange messages through the website. Participants could also earn game points for completing their profile, following other players, and referring friends. These features were designed to inspire website interactivity, boost authentication attempts, and create a natural sense of realism and actual privacy risk.

To make the game points relevant and desirable to participants, we provided weekly and end-of-game rewards. Each week, we awarded five to 15 $10 gift cards to the participants who either (1) were first to find all of that week's locations, or (2) were randomly selected based on a point-weighted virtual "drawing." At the end of the game, the two participants with the most total points, and one more based on a point-weighted random drawing, won a new tablet computer.

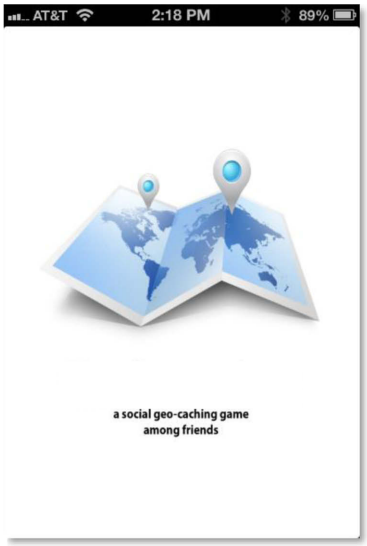
3.1. Ensuring Experimental Validity

Five hundred and sixty-eight undergraduates at a large private university in the western United States participated in the experiment. To generate valid and realistic information disclosure behaviors, participants needed to perceive actual personal risk and fear of disclosing information. This was accomplished in multiple ways. First, we obtained IRB[2] approval to *not* require participants' informed consent because informed consent automatically elevates participants' awareness of risk and the artificial nature of data collection. Rather, participants were recruited under the false pretense that a local mobile app business wanted to pilot test a new geo-caching app at their university. As a result, there was no priming effect on participants and they were less susceptible to social desirability bias (Richman et al. 1999). Moreover, they were told that the friends they referred to the game did not have to be university students or employees.

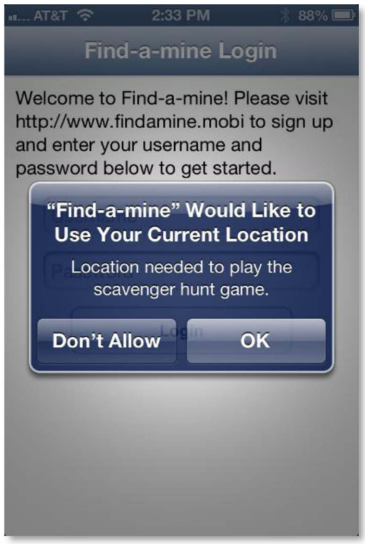
[2] Universities in the U.S. require research involving human subjects to be approved by an Institutional Review Board (IRB) to ensure that participants do not suffer physical or psychological harm. Normally, this involves fully explaining the nature of the experimental treatments and obtaining informed consent.

Figure 5 **(Color online) Mobile App Screenshots**

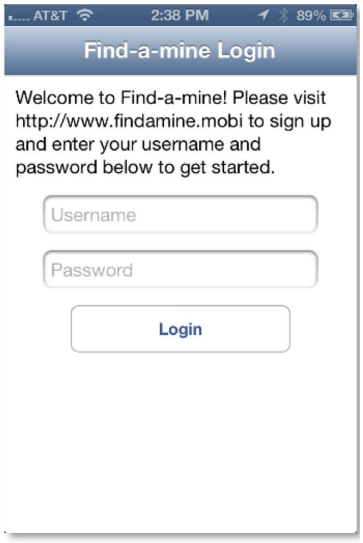
(a) Splash screen



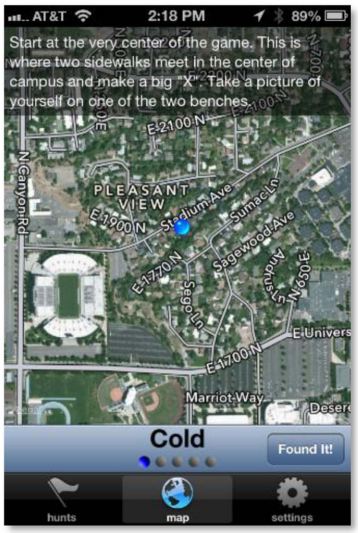
(b) Location data disclosure



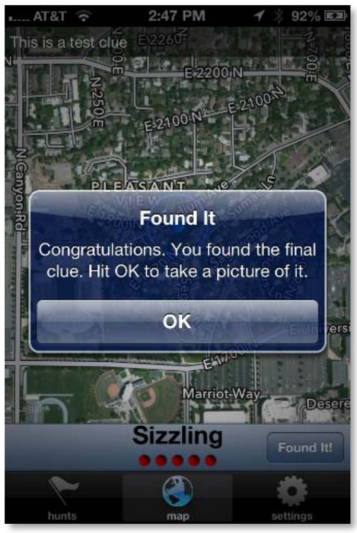
(c) Mobile app login



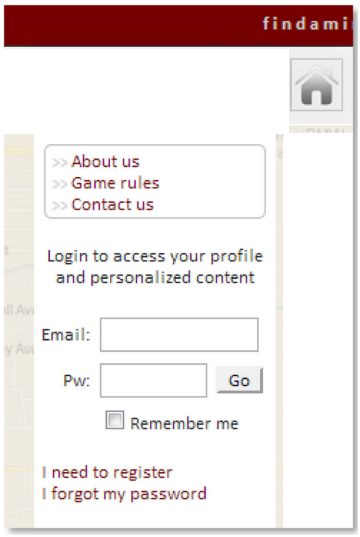
(d) Clue begins



(e) Mobile app clue found



(f) Desktop website login Web part



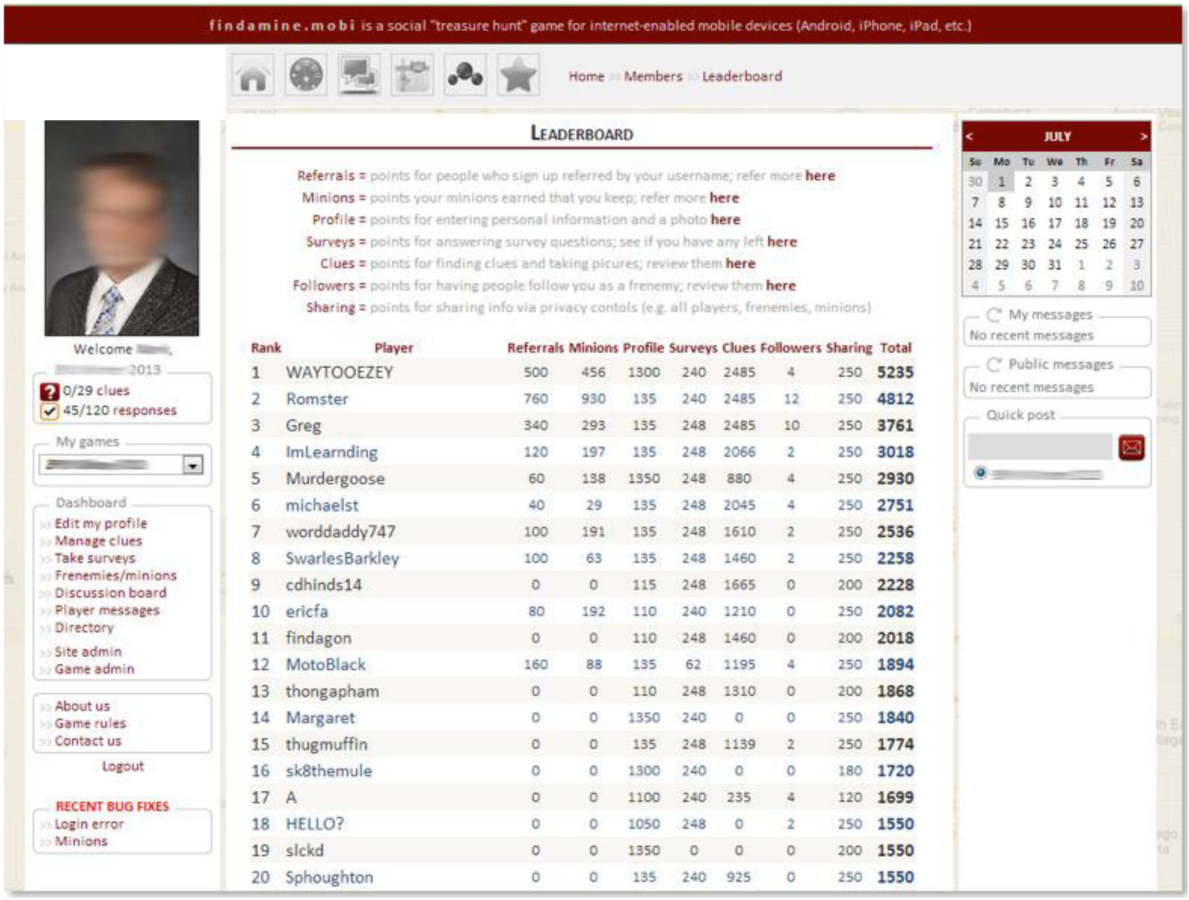
Second, the context of the app was chosen to replicate several relevant forms of information privacy and encourage consistent disclosure. For example, by choosing an app design with weekly incentives, participants were motivated to play for more than just extra credit. Because it was a geo-caching app, there was a clear need to collect location data, which presents personal safety risks (Baum et al. 2009). The social network aspect of the app created both additional enjoyment as well as creating vertical and horizontal personal information privacy risks (Posey et al. 2010). Thus, participants' personal information could legitimately be made publicly available—unless they set their privacy settings to restrict their data to "friends only" or "nobody." This is critical because fear is essential to motivating users to create strong passwords (Vance et al. 2013).

Third, the findamine app architecture needed to match those that are most potentially dangerous. In particular, the game was made possible by a native mobile app, a cross-platform website, and Web services that connected the mobile app to the external database. This common architecture allows mobile apps to easily send data to external third-party servers. When the app was introduced to participants, they were given a brief explanation of how the mobile app and website worked together with the same data. Consequently, participants were aware that the mobile app was capable of sending personal information to remote servers.

3.2. Experimental Manipulation

The study's objective is to investigate the effect of the UI on people's behavior when using authentication

Figure 6 (Color online) Game Leaderboard (Desktop Website View)



credentials of different types and strength. Prior research has found that people do not voluntarily create long passphrases (Keith et al. 2007, 2009). Therefore, we manipulated the instructions in an attempt to encourage some participants to create and use passphrases.

Participants were randomly assigned to one of three conditions when they opened the website.[3]

1. Control group: no instructions or requirements for credential generation.

2. Passphrase group: passphrases encouraged, but not required through technical verification (to estimate real voluntary use).

3. Passphrase + benefit group: passphrases encouraged and users told they would not be required to change their credential as often.

3.3. Measures

Because of our research design, we were able to capture a variety of valid and objective measures for credential characteristics, coping behaviors, and task success.

3.3.1. Credential Strength. The appendix describes several possible measures of credential strength and the reasons that led us to select experts' subjective assessment to test our hypotheses. Consistent with prior research (Keith et al. 2007, 2009), we measured credential strength by providing the actual authentication credentials to two coders[4] who were unaware of the study's hypotheses and asked them to make a subjective judgment as to whether the credential was "simple," "moderate," or "complex" in terms of strength against cracking attempts. Because complex passwords do not follow traditional spellings and language patterns, they are also more resistant to guessing and "cracking." As a result, the concept of complexity is essentially synonymous with credential strength (Adams et al. 1997, Keith et al. 2009) in the password context. Therefore, the coders were instructed to interpret these terms as being indicative of the likelihood that the credential could be

[3] It should be noted that the purpose of this study is not to test the efficacy of credential instructions. The purpose of the instructions was to encourage the creation of different types of credentials to facilitate testing our hypotheses.

[4] One coder was a master's student in IS with an emphasis in security. The other coder is a vice president of operations at a large consumer information privacy company.

guessed by a human or program. To further guide their subjective assessments, they were briefed on the objective experimental findings from prior research (Keith et al. 2007, 2009) on the proven characteristics of strong credentials (e.g., length and character variance). These coders agreed on 81% of the credential ratings ($K = 0.813, p < 0.001$). When the coders disagreed, we deferred to the practitioner. We used this three-level (simple–moderate–complex) subjective assessment to represent the strength of a participant's initial authentication credential.[5]

3.3.2. Login Failures. Actual login failures were measured to represent the environmental impacts in Figure 2. Every login attempt was captured in the database and coded to reflect the outcome of that attempt (success or failure).

3.3.3. Longitudinal Authentication Behaviors. We captured two types of longitudinal authentication behaviors. First, for each login attempt we recorded whether the user entered their credential manually or avoided entry by using the "remember me" feature. Higher scores represent a greater percentage of all authentication attempts were performed with a saved credential—thus indicating less secure authentication behavior. Second, we stored every credential a user ever created and had the two judges rate both the initial and changed credentials. We calculated the change in credential strength by subtracting the rating of the old credential from the rating of the new. Both ratings were on three-point scales (simple, moderate, complex), so the change score could range from −2 to +2.[6] Thus, negative scores reflect changing to a weaker credential, and positive scores reflect changing to a stronger credential.

3.3.4. Mobile Interface and Mobile Practice. To test the effects of the UI and practice we collected data about the client browser and operating system information at each login attempt to determine whether the login was from a mobile device or a traditional laptop or desktop computer. We created a variable called mobile interface by calculating the percentage of all login attempts made using a mobile device. However, this does not distinguish between a user who only made two login attempts total with one being from a mobile device and a user who made 20 login attempts, with 10 from a mobile device. Therefore, to differentiate between these two types of users, we also calculated the raw count of attempts over a mobile device as a measure of overall mobile practice.

3.3.5. Control Variables. Three control variables were included in the analysis. First, the total number of login attempts was used to control in predicting the total number of login failures and the number of successful login attempts based on a stored password. Second, two demographic variables—age and gender—were collected from the findamine.mobi profiles as used as controls for login failures, storing credentials, and changing credentials.

Table 1 Descriptive Statistics

	Male ($n = 402$)	Female ($n = 166$)
Age (years)	$\bar{x} = 23.46$	$\bar{x} = 20.91$
Points accumulated	$\bar{x} = 1{,}569$	$\bar{x} = 1{,}425$
Weekly prizes won	55 (76.4%)	17 (23.6%)
Friends recruited	162 ($\bar{x} = 0.61$)	25 ($\bar{x} = 0.30$)
Number of website sessions	Total $\bar{x} = 9.90$ Mobile $\bar{x} = 3.90$	Total $\bar{x} = 4.79$ Mobile $\bar{x} = 1.43$

Table 2 Type of Credential Created

Treatment	Password	Passphrase
1. No prompt (control) (%)	91	9
2. Passphrase prompt (%)	81	18
3. Passphrase + Benefit (%)	85	15
Gender (of those who disclosed)		
Male	277	52 (16%)
Female	141	24 (15%)

4. Result

4.1. Descriptive Statistics

Table 1 presents descriptive statistics of the players (demographic data were recorded from the player's game profile) and their gameplay. About two-thirds (68%) of participants were male. Although participants could refer any friend to play the game to earn points, men comprise a larger portion of the electronic gaming population (ESA 2013) and even more so of geocachers (Schneider et al. 2011).

Table 2 indicates the number of passwords versus passphrases created by group manipulation. An ANOVA including contrast estimates indicate that treatment 2 ($p = 0.03$) was successful because players in that condition were more likely to create a passphrase than were players who were not prompted to consider doing so. Interestingly, treatment 3 resulted in fewer passphrases created than treatment 2. There was no gender difference in credential selection.

Table 3 shows descriptive statistics about the length, character set, complexity, and strength of participants' authentication credentials. Strong credentials

[5] Reanalysis of our data using several composite measures of credential strength yielded substantially the same results. Therefore, in the interest of simplicity, we report analysis based on experts' judgments of credential strength.

[6] For example, changing from a complex to a simple credential would yield a change score of −2 (1 − 3), whereas changing from a complex to a moderate strength credential would yield a change score of −1 (2 − 3).

Table 3 Credential Strength Details

	Simple	Moderate	Complex	Overall
Average entropy (bits)	47.87	60.83	79.73	54.4
Percent cracked	66.59	22.23	13.73	54.72
Key presses required for traditional UI	9.17	11.54	13.72	10.14
Key presses required for mobile UI	10.05	13.40	14.42	11.07
Count	424	48	96	568

had higher theoretical entropy, were more difficult to crack, and required a greater number of key presses than either simple or moderate strength credentials (see the appendix for details). However, most credentials were simple and quickly cracked.

Table 4 summarizes descriptive statistics about credential use. Participants attempted to log in from a laptop or desktop more often than from a mobile device (1,612 versus 1,022 attempts). However, 194 (34%) of participants logged into the website via their mobile device at least once, with almost 39% of all website access occurring via mobile device. Login failures were more likely when using a mobile device. Two hundred and eighteen (38%) participants stored their credentials, with storage being more likely when using mobile devices. Seven percent of participants changed their credentials a total of 45 times. Overall, the tendency was to change to a weaker credential: eight participants changed from a complex to a simple credential (change score of −2) and 16 changed from either complex to moderate or moderate to simple (change scores of −1), but only five people switched to a stronger credential. There was no significant difference between passwords (36.2%) and passphrases (35.7%) in terms of storing the credential or changing to a credential that was either weaker or of the same strength (6.5% each).

4.2. Tests of Hypotheses

We analyzed a path model with the partial least squares (PLS) structural equation modeling (SEM) technique using SmartPLS 3.0 (Ringle et al. 2014) to test our hypotheses. The use of PLS is appropriate because (1) we need to test multiple paths in the same model, (2) most of our measures are not interval based, and (3) several of our measures do not exhibit a normal distribution (Chin et al. 2003, Fornell and Bookstein 1982). Figure 7 shows the PLS model we used to test our hypotheses. Interaction effects were tested using the product-indicator approach (Chin et al. 2003). Table 5 lists the path coefficients for covariates that were tested in our model, but which are omitted from Figure 7 so that it focuses on our hypotheses. The R^2 values indicate the variance explained in that construct.

Table 5 PLS Path Loadings Not Depicted in Figure 7

Path	Coefficient	*t*-stat
Gender → Login failures	−0.054	1.28
Gender → Storing credential	−0.011	0.53
Gender → Changing credential	−0.016	0.58
Age → Login failures	0.040	0.92
Age → Storing credential	−0.037	1.36
Age → Changing credential	−0.019	0.84
Total login attempts → Login failures	0.279	1.26
Total login attempts → Storing credential	0.632	2.16*

$^{\dagger}p < 0.10$; $^{*}p < 0.05$; $^{**}p < 0.01$; $^{***}p < 0.001$.

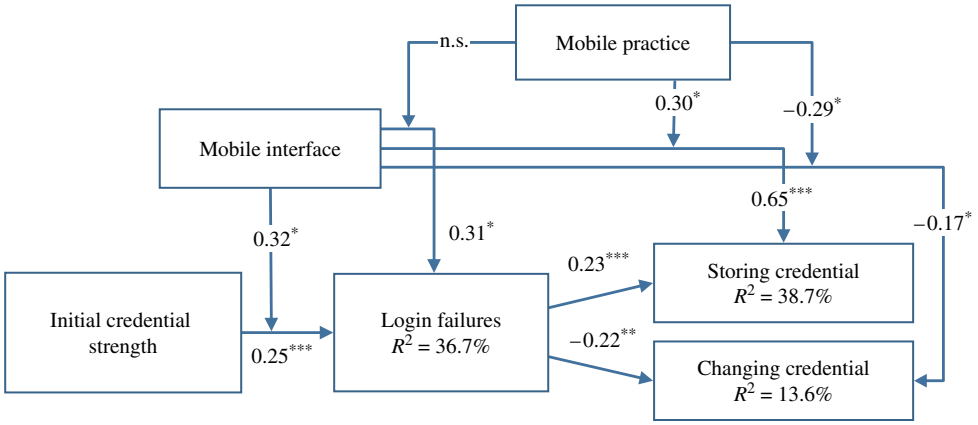
H1 predicted that stronger authentication credentials would increase login failures due to typing errors and memory failures. Figure 7 shows that, after controlling for login attempts, the path from credential strength to login errors is significant and positive ($\beta = 0.254, p = 0.001$). Thus, H1 is supported. H2 predicted that login failures would be higher when using a mobile UI than when using a full-size physical keyboard. The path from the use of a mobile device to login failures is positive and significant ($\beta = 0.305, p = 0.041$). Thus, H2 is supported. H3 predicted that the effect of credential strength on login failures would be greater when using a mobile UI than when using a full-size physical keyboard. Figure 7 also shows that the use of a mobile device had a significant, positive moderating effect on the effect of credential strength on login errors ($\beta = 0.319, p = 0.027$). Thus, H3 is supported.

H4A and H4B predicted that login failures would lead to the adoption of less secure authentication behavior, either by storing the authentication credential or changing to a weaker one. As shown in Figure 7, the path from login failures to storage of

Table 4 Credential Use Behaviors

	Simple	Moderate	Complex	Total
Total mobile login attempts	744	139	84	1,022
Total traditional login attempts	1,074	361	177	1,612
Mobile login failure rate (%)	18.54	42.27	33.33	24.31
Traditional login failure rate (%)	18.62	25.76	23.73	20.78
Mobile remembered login rate (%)	44.89	40.72	42.86	43.85
Traditional remembered login rate (%)	31.28	26.87	48.59	32.20
Count of changes to each type	$n = 32$	$n = 12$	$n = 1$	$n = 45$
Count of changes away from each type	$n = 15$	$n = 20$	$n = 10$	$n = 45$

Figure 7 (Color online) PLS Path Coefficients



Notes. Gender and age are not depicted for simplicity.
*$p < 0.05$; **$p < 0.01$; ***$p < 0.001$.

the credential is significant and positive ($\beta = 0.226$, $p < 0.001$), indicating that login failures increased the tendency to store authentication credentials. The path from login failures to changing credentials is negative and significant ($\beta = -0.222$, $p = 0.009$), indicating that login failures result in changing to a weaker credential. Thus, both H4A and H4B are supported. Overall, 230 (40%) participants either stored their credential or changed it.

H5A and H5B predicted that use of a mobile UI would increase the likelihood of less-secure authentication behaviors by either storing their authentication credentials or switching to a credential that is simpler to use but weaker. As shown in Figure 7, the path from mobile device use to storage of credentials is positive and significant ($\beta = 0.654$, $p = 0.001$), indicating that as the proportion of access attempts via mobile devices increases, so does the tendency to store the authentication credential. Figure 7 also shows that the path from mobile device use to entropy of the new credential is negative and significant ($\beta = -0.166$, $p = 0.024$), indicating that increased use of mobile devices increases the tendency to switch to a weaker credential. Thus, H5A and H5B are supported.

We also explored whether practice ameliorates the impact of using a mobile UI on login failures and coping behaviors. Figure 7 shows that practice does not significantly moderate the path between mobile device use and login failures ($\beta = -0.093$, $p = 0.248$), but does affect both the likelihood of storing authentication credentials ($\beta = 0.295$, $p = 0.033$) and the tendency of mobile device users to change to a weaker authentication credential ($\beta = -0.291$, $p = 0.050$). However, the signs of the coefficients are mixed, indicating that practice affects the two coping behaviors in different ways. The sign of the coefficient on the path representing H5A is positive, indicating that increased practice exacerbates, rather than mitigates, the tendency to store authentication credentials when using mobile devices. By contrast, the sign of the coefficient on the path representing H5B is negative, indicating that practice ameliorates the tendency to switch to a simpler credential.

Finally, we also examined demographic factors. Neither gender nor age affected login failures, the likelihood of storing credentials, or the likelihood of switching to a weaker credential.

5. Discussion

This study extends research on voluntary security behaviors by investigating the factors that influence their (dis)continuance. Drawing on the *process* portion of the TTAT proposed by Liang and Xue (2009), we find that the decision to (dis)continue a security behavior emerges from a cybernetic loop that reflects one's experience in performing that behavior. In other words, although users may initially adopt a secure behavior, they will modify or drop that behavior if it requires too much effort to perform successfully. Specifically, we found that when a strong authentication credential results in login failures, people tend to either store their authentication credential for auto-submission or to change to a credential that is easier to enter correctly. Both solutions solve the problem of login failures, but do so at the cost of weakening security. Thus, we show that the IT artifact (the nature of the user interface for entering authentication credentials) affects both the success in executing a security behavior and the decision to (dis)continue that behavior. Our findings have important implications for both research and practice.

5.1. Implications for Research

Overall, our results show that a longitudinal and process-oriented perspective is essential to understanding how the IT artifact, specifically the nature

of the user interface, affects user security behaviors. We found a clear cycle of behavior based on temporal introduction of different stimuli. Initially, users create authentication credentials that reflect their desire for a given level of security. Subsequently, after users practice a security behavior (by attempting to login through a prompt), their behaviors reflect a desire for usability: if their initial authentication credential is too difficult to correctly enter via the UI of a mobile device they either configure the device to store and automatically submit the credential or they change to a simpler, but weaker, one.

From a theoretical perspective, these findings support cybernetic loop theory (Carver and Scheier 1982) as a process model of security behavior continuance. We thus extend the process version of Liang and Xue's (2009) TTAT to show that cybernetic processes not only explain how people respond to a threat but also account for how the IT artifact affects their security behaviors. We further contribute to this theory by drawing from research on memory systems (Ullman 2004), IS research on the effect of cognitive load on decision strategy (Todd and Benbasat 1991, 1992, 1999), and psychology research on the role of emotions in decision making (Bargh and Ferguson 2000, Bargh et al. 2001, Chen and Bargh 1999) to explain how the cybernetic loop process model will unfold in the context of authentication security goals and behavior. In particular, two user goals independently and jointly influence the continuance of secure behaviors over time and cause people to enter additional cycles of the cybernetic feedback loop. The first goal is the user's desire for security, which is currently well explained by variance models such as TTAT (Liang and Xue 2009) and adapted *protection motivation*-based theories (Johnston and Warkentin 2010, Herath and Rao 2009). The second goal is the user's desire for usability, which is affected by the nature of the IT artifact (UI) used to perform the task. However, these two goals are not simultaneously considered (e.g., in a cost/benefit trade-off calculation) each time a user must make a decision about their security behaviors. Rather, consideration of the security goal is stimulated by events such as security training and awareness programs (Bulgurcu et al. 2010) or personal experience with security breaches (Herath and Rao 2009), whereas the usability goal is stimulated by difficult experiences with maintaining the security behavior as a person interacts with the IT artifact. Therefore, a theoretical process model that accounts for behavioral adjustments over time best explains behavior.

Our findings also underscore the importance of acknowledging human factors issues, specifically ease of use, as an *inhibitor* of secure behavior. Just as people are often willing to trade off accuracy for effort when making decisions (Todd and Benbasat 1991, 1992, 1999), our results show that they are willing to trade off security for ease of use. Thus, in our experiment, when people experience repeated login failures when using mobile devices, they respond by switching from a more secure authentication behavior (i.e., manual entry of a strong credential) to less secure, but easier to perform alternatives (use of a simpler credential or storage and autosubmission of the credential).

Clearly, there is a need for further theory development and research that focuses on usability when using mobile devices in the authentication process. Prior research on authentication credentials when using physical keyboards provides an example of the kind of approach that is needed. Keith et al. (2007) found that long passphrases which did not reflect well-learned typing skills resulted in login failures. Building off that finding, Keith et al. (2009) hypothesized and found that simple instructions to create passphrases that used basic rules about typing (e.g., capitalization of initial letters of words, use of numbers as parts of dates, etc.) would make such credentials easier to use. In this study, we found that stronger authentication credentials increased login failures. An important topic for future research is to investigate how to design credentials that are strong, yet easy to correctly enter when using mobile devices with virtual touchscreens.

Our results also suggest that improving user memory systems (i.e., practice) is not a panacea for the limitations of mobile interface. Although practice did decrease the propensity to switch to weaker credentials when using a mobile device to authenticate, it did not reduce the login failure rate when using a mobile device. Moreover, contrary to expectations, continued practice with the mobile UI to authenticate actually *increased* the propensity to store those credentials. We propose that these three findings are interrelated. The finding that practice did not reduce login failures suggests that entering a password over a mobile UI never became as easy as when using a traditional keyboard and full-sized screen. As explained before, the mobile UI still requires many more keystrokes for the same text (Jakobsson and Akavipat 2012) even if every keystroke is correct. Therefore, the repeated practice of authentication over a mobile UI may have been simply a stark reminder of the extra effort required to enter a strong credential with such a UI, and the concomitant increase in the likelihood of making mistakes. If we are correct that the problem is caused by the nature of the UI, it is logical that users would respond by adopting the coping behavior that resolves the problem by eliminating the need to manually enter the credential—thus, mobile UI practice leading to an increased likelihood of storing the password—rather than the coping behavior

that still required manual entry of the credential. However, although plausible, we cannot support this explanation with our data and, therefore, suggest that it is an important topic for future research.

5.2. Implications for Practice

Although our study investigates voluntary security behavior, our findings are relevant to the workplace. Employers are increasingly allowing employees to use their own personal mobile devices to access the corporate network, a practice referred to as "bring your own device" (BYOD). Over time and through repeated experience, people develop habits on how they use technology (Limayem et al. 2007). If employees get habituated to acting in a certain way when using mobile devices for personal use, those habits may carry over when using that same personal mobile device for work.

On the surface, the move to use mobile devices to authenticate to remote systems appears likely to improve security because it involves multifactor authentication using a combination of something you have (your mobile device) and something you know (a PIN, password, or passphrase). However, our results suggest that the inherent design features of the mobile UI may actually *decrease* security because users are likely either to change from a strong, but hard-to-enter, credential to a weaker, but easier to enter, one or to store their credential on the device and configure it for autosubmission (thus changing what appears to be multifactor authentication to multimodal authentication using two things that a person has: their mobile device and the stored credential). However, mobile devices are susceptible to being lost or stolen; over three million smartphones were stolen in 2013 (ConsumerReports 2014). In addition, people sometimes "loan" their phone to others (Ben-Asher et al. 2011, Karlson et al. 2009). In either case, this increases the risk that whoever has obtained physical possession of the device can attempt to gain unauthorized access to the corporate system. This risk is further increased by the fact that survey data indicate that a majority of companies that currently permit BYOD rely *solely* on passwords for authentication (Johnson and DeLaGrange 2012).

One potential solution to this problem is for people to configure their mobile devices to require authentication to turn it on. Disturbingly, survey results find that many people do not configure their phones to require any form of authentication (Clarke and Furnell 2005, ConsumerReports 2014, Jones and Heinrichs 2012). Moreover, the majority of people who do configure a password or PIN to access their phone report that they *never* change it (Barn et al. 2014). The trend to incorporate biometrics to initially logon to a mobile device (e.g., fingerprints or facial recognition) mitigates the risk that an unauthorized person can use a lost or stolen device. However, the threat is not totally eliminated because (1) it is still possible for people to configure their device to bypass such controls; (2) the device could be left unattended and stolen after the owner used the biometric to turn it on; and (3) the owner would definitely have to have authenticated prior to "loaning" the device to another person.

Thus, managers need to be concerned about how BYOD might affect employees' choice and use of authentication credentials. Of course, employers will probably require employees to configure their mobile devices to require authentication as a condition of permitting BYOD. Employers will also create and enforce policies regarding the need to periodically change passwords. Consequently, the important question is the extent to which employees truly comply with those policies or attempt to circumvent them, for example by storing their credential and configuring their mobile device to automatically submit it whenever they want to login to the corporate system, to make life easier. Our results suggest that this is indeed a potential problem.

In summary, our results have implications for both managers and users. Managers need to reconsider how they formulate security policies and deploy new IT artifacts. It is not enough to focus only on how a new technological development or a proposed policy, if properly implemented and complied with, improves security. Managers must also consider how changes in the IT artifact (e.g., replacing a full-size physical keyboard with a virtual touchscreen) and policy requirements (e.g., password credential composition rules) interact with one another in the context in which they will be used. In particular, our results suggest that (1) secure authentication policies that are effective in the desktop computing paradigm will not work in the mobile paradigm, and (2) voluntary secure authentication behaviors that are not adequately usable *will* be discontinued. Therefore, managers must ensure that a secure authentication policy is sufficiently usable or at least find ways to force users to comply with it. Otherwise, they risk having their employees develop "creative workarounds" that make it easier to "comply" with policies, but in a manner that actually reduces security. Similarly, users should be wary of our natural tendency to place usability before security and exercise safe judgment in spite of mobile UI limitations.

5.3. Limitations

This study is subject to several limitations inherent with the use of student subjects in a controlled experiment. One issue concerns the extent to which the results generalize to other populations of interest.

It is possible that age and experience with mobile devices may affect our results. However, as noted earlier, we did test for and failed to find evidence that repeated practice in using a mobile device to authenticate ameliorated the login failure rate or the tendency to switch to a simpler credential. Moreover, if it is true, as it is sometimes argued, that younger people have fewer problems using IT than do older people, then the use of students as subjects may actually understate the magnitude of the problems associated with using complex authentication credentials to log in via mobile devices.

Another issue is that controlled experiments may cause participants to behave differently than they would in real situations. As we explained when describing our research design, we took several steps to mitigate that risk, including obtaining permission to not inform participants that this was an experiment. In addition, we designed the experiment so that participants believed that they were playing a game. Gamification has been shown to cause people to become absorbed in the immediate task (i.e., playing the game) and, thereby, to reveal more realistic behaviors (Agarwal and Karahanna 2000, Deterding 2012, Hoffman and Novak 1996, Singh 2012). Furthermore, the game data stored in their findamine profile had strategic value in the context of the game itself: a player who accessed other players' accounts could view their clues about the target locations. Therefore, much like a poker player needs to keep their cards private, findamine players needed to keep their clues private, which should have motivated them to restrict access to those data via use of a strong authentication credential. There was also an element of personal risk associated with unauthorized access to their personal information. Although findamine did not include credit card or bank account information, it did record and share their GPS location, social network connections, and demographic profile data similar to that found in major online social networks. Disclosure of GPS information enables criminals to stalk victims, which can lead to robberies when the victim is not home (Johanson 2013) or serious physical crimes such as assault, rape, or murder (Baum et al. 2009, HuffingtonPost 2012). In summary, we believe that our participants were motivated to participate in a variety of ways for an assortment of reasons.

One potential source of variance not accounted for in our study is that mobile users may employ an external keyboard when using their device.[7] It was not possible to capture this nuance in the client variables we recorded in each login attempt. However, such behavior by participants in our study would only bias against finding any difference in login failure rates due to different UI.

[7] We thank an anonymous reviewer for raising this issue.

The design of our experiment did not permit us to collect data to determine whether the reason that participants discontinued a strong authentication behavior was primarily cognitive (i.e., a conscious attempt to reduce effort) or emotional (dissatisfaction or annoyance). However, both explanations are consistent with predictions based on cybernetic loop theory that people will respond to repeated login failures by discontinuing a behavior that leads to task failure. We leave exploration of this issue as a topic for future research.

Finally, we drew on existing knowledge about memory systems to derive implications concerning the effect of the UI on the continuance of secure behavior. However, our understanding of how memory systems function is continually evolving (Baddeley 2012). Therefore, IS security researchers need to monitor new insights from psychology research on memory because those findings may suggest even more effective ways to design the UI to best support secure behaviors.

6. Conclusions

This paper reports the results of a field experiment that investigated the effect of an IT artifact (the nature of the UI) on authentication behaviors. Our most important finding is that user authentication behaviors differ depending on whether they are using traditional computers or mobile devices for remote access to a network. We demonstrate that those differences are due to differences in the UI of the two types of devices. Thus, our study underscores the need for security researchers and practitioners to consider how the IT artifact interacts with task characteristics (e.g., requirements about authentication credential composition) when considering the effects of adopting new technologies or changing security requirements. As Adams and Sasse (1999, p. 40) argue, "users are not the enemy" but only create problems because of mismatches between human capabilities and the requirements of secure behavior.

Acknowledgments

The authors would like to sincerely thank the review team for the time and effort they gave to greatly improve the quality of this paper. The authors would also like to thank the reviewers and participants of the 2013 Dewald Roode Information Security and Privacy Workshop IFIP WG8.11/WG11.13 for their constructive comments and suggestions. Any remaining mistakes are the sole responsibility of the authors.

Appendix. Details of Credential Strength Measures

Credential composition and strength was measured in a variety of ways. First, the theoretical entropy was calculated: Entropy $= \log_2 N^L$, where N is the size of the character set and L is the length (Bialynickibirula

Table A.1 Pearson Correlation Table

	Entropy	Cracked
Cracked	−0.39***	
Expert judgment	0.54***	−0.32***

***Significant at the $p < 0.001$ level.

and Mycielski 1975). Entropy represents the difficulty of attempting a brute-force approach to guessing a credential, with higher levels of entropy indicating a "stronger" credential. Entropy is considered a more accurate measure of true credential strength against cracking than merely calculating the total number of possible password combinations based on a given length and character set, N^L (Johansson and Riley 2005) because the length of a password, in bits, plus the size of the character set, creates a doubling of the number of guesses required for brute-force cracking for each bit added to the password information.

However, credential entropy is still only a hypothetical measure of strength. The actual words and word permutations commonly used in credentials, and also found in rainbow tables,[8] is constantly changing based on user behavior. Therefore, we created NT hashes[9] of each password used and then used two separate programs to see which credentials could be cracked. The first program was an open-source program called Ophcrack. All of the free rainbow tables that came with Ophcrack were used. The other program was a private paid application called Hash Suite with more advanced rainbow tables. The second measure of credential strength (i.e., initial coping behavior) was whether the user's credential could be cracked by either of these programs. Both entropy and credential crack rate are summarized by credential type in Table 3.

Because both of the objective measures listed above contain known potential measurement and error issues, we also considered experts' assessment of credential strength, a subjective measure used in prior research (Keith et al. 2007, 2009). We recruited two independent expert judges—who had no part or stake in the outcome of the research—to rate each credential's complexity and strength as "simple," "moderate," or "strong." These coders agreed on 81% of the credential ratings ($K = 0.813, p < 0.001$). When the coders disagreed, we chose to use the decision by the expert practitioner.

Table A.1 shows that all three measures were correlated with one another. Both entropy and expert judgment are negatively correlated with cracked. Thus, as expected, credentials with higher entropy are less likely to be cracked. Similarly, credentials judged to be complex are less likely to be cracked than credentials that experts assessed as being simple.

Table A.1 also shows that entropy and expert judgment are positively correlated, but apparently also measure different aspects of credential strength. Therefore, we investigated how well each measure related to whether a particular credential was likely to be cracked. Table A.2 lists several example passwords[10] and their subsequent entropy scores, expert ratings, and whether or not it was successfully cracked.

Table A.2 Example of Credential Strength Results

Credential	Entropy	Expert	Cracked
password	40.00	1	Yes
wrosapsd	40.00	2	No
icecreamsandwhich	88.56	2	Yes
Extra8iscuit$	81.95	3	No
icanfind	40.00	2	No
Basketball11	73.55	2	Yes

Notes. Expert scores: 1 = simple; 2 = moderate; 3 = complex.

Note that the first two passwords (password and wrosapsd), have the exact same entropy scores because they are of the same length and are derived from the same character base (lowercase letters). However, the expert judged the latter to be moderately complex (2) but considered the former to be simple (1), and those judgments were consistent with the fact that "wrosapsd" was not cracked, whereas "password" was.

Now consider the second two passwords: "icecreamsandwhich" has a higher entropy score than does "Extra8iscuit$" because of its length, but "Extra8iscuit$" comes from a larger character base that includes both uppercase and lowercase letters, numbers, and characters. Once again, the expert correctly judged "Extra8iscuit$" to be more complex: it was not cracked, but "icecreamsandwhich" was.

The last two passwords represent a situation where the password cracking software was a poor indicator of complexity because it was able to crack the higher entropy password of "Basketball11" but not the lower entropy password of "icanfind." This is because the success of the cracking software depends on the quality of the rainbow tables. If the rainbow table is poor, then the cracking results will also be poor. In this case, the expert judged both passwords to be moderately complex (2): "icanfind" because it was a phrase and not a single word; "Basketball11" because it contained multiple types of characters and was longer even though it was a single word.

These three examples suggest that expert judgment is likely a better indicator of true credential strength than entropy scores. We think that one reason for this difference is that the chance of login failures increases with the number of keystrokes required to enter a credential, but the entropy scores for two credentials may not be related to the number of keypresses required to enter that credential. For example, refer back to the second pair of credentials in Table A.2. The first, "icecreamsandwhich" has an entropy

[8] A rainbow table is a precomputed list of password hashes usually used for recovering/cracking plain-text passwords.

[9] An NT hash refers to the algorithm used by Windows operating systems to generate hashed versions of user passwords.

[10] Other than the password "password," all other credentials in this table were modified slightly to comply with IRB restrictions. However, the examples were modified to reflect the same entropy score as the original credential (i.e., the nonword "wrosapsd" replaces an actual credential that was a nonword comprised of eight lowercase alphabetic characters). Moreover, the expert rating and cracked status are based on the actual credential.

score of 88.56 and requires 17 keypresses to enter; the second, "Extra8iscuit$" has a lower entropy score of 81.95 but also requires 17 keypresses to enter on a virtual touchscreen interface. Entropy scores also do not take into account the *nature* of keypresses. The 17 keypresses required to enter "icecreamsandwhich" each only require pressing one finger at a time on a physical keyboard. They also require pressing only one key at a time on a virtual touchscreen, without the need to ever shift displays. By contrast, entering the credential "Extra8iscuit$" on a physical keyboard requires pressing two keys simultaneously twice (shift plus e to yield E, and shift plus 4 to yield $). On a virtual touchscreen, it requires changing the display five times (once to shift to capital letters, once to return to lowercase, once to change to numbers, once to return to lowercase, and once to display special symbols including the $). We believe that the need to either press multiple keys simultaneously on a physical keyboard or the need to continually press a key to change the display on a virtual touchscreen increases the probability of a typing mistake. Therefore, based on the preceding discussion, and to be consistent with prior research on the use of authentication credentials (Keith et al. 2007, 2009), we chose to use expert judgment as our measure of credential strength.

References

Adams A, Sasse MA (1999) Users are not the enemy. *Comm. ACM* 42(12):40–46.

Adams A, Sasse MA, Lunt P (1997) Making passwords secure and usable. Thimbleby H, O'Conaill B, Thomas PJ, eds. *People and Computers* XII (Springer, London), 1–19.

Agarwal R, Karahanna E (2000) Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS Quart.* 24(4):665–694.

Anderson CL, Agarwal R (2010) Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quart.* 34(3):613–643.

Baddeley A (1994) The magical number seven: Still magic after all these years? *Psych. Rev.* 101(2):353–356.

Baddeley A (2012) Working memory: Theories, models, and controversies. *Annual Rev. Psych.* 63:1–29.

Bao P, Pierce J, Whittaker S, Zhai S (2011) Smart phone use by non-mobile business users. Bylund M, Juhlin O, Fernaues Y, eds. *Proc. 13th Internat. Conf. Human Comput. Interaction Mobile Devices Services* (ACM, New York), 445–464.

Bargh JA, Ferguson MJ (2000) Beyond behaviorism: On the automaticity of higher mental processes. *Psych. Bull.* 126(6):925–945.

Bargh JA, Gollwitzer PM, Lee-Chai A, Barndollar K, Trötschel R (2001) The automated will: Nonconscious activation and pursuit of behavioral goals. *J. Personality Soc. Psych.* 81(6): 1014–1027.

Barn BS, Barn R, Tan J-P (2014) Young people and smart phones: An empirical study on information security. Sprague RH Jr, ed. *Proc. 47th Hawaii Internat. Conf. System Sci.* (*HICSS*) (IEEE, Los Alamitos, CA), 4504–4514.

Baum K, Catalano S, Rand M (2009) National Crime Victimization Survey: Stalking Victimization in the United States–Revised NCJ 224527, Bureau of Justice Statistics Special Report, U.S. Department of Justice, Office of Justice Programs, Washington, DC. http://www.bjs.gov/content/pub/pdf/svus_rev.pdf.

Belanger F, Crossler RE (2011) Privacy in the digital age: A review of information privacy research in information systems. *MIS Quart.* 35(4):1017–1041.

Ben-Asher N, Kirschnick N, Sieger H, Meyer J, Ben-Oved A, Möller S (2011) On the need for different security methods on mobile phones. Bylund M, Juhlin O, Fernaues Y, eds. *Proc. 13th Internat. Conf. Human Comput. Interaction Mobile Devices Services* (ACM, New York), 465–473.

Bhattacherjee A (2001) Understanding information systems continuance: An expectation-confirmation model. *MIS Quart.* 25(3):351–370.

Bhattacherjee A, Premkumar G (2004) Understanding changes in belief and attitude toward information technology usage: A theoretical model and longitudinal test. *MIS Quart.* 28(2): 229–254.

Bialynickibirula I, Mycielski J (1975) Uncertainty relations for information entropy in wave mechanics. *Comm. Math. Phys.* 44(2):129–132.

Brown AS, Bracken E, Zoccoli S, Douglas K (2004) Generating and remembering passwords. *Appl. Cognitive Psych.* 18(6):641–651.

Brown RM, Robertson EM (2007) Off-line processing: Reciprocal interactions between declarative and procedural memories. *J. Neuroscience* 27(39):10468–10475.

Brown SA, Venkatesh V, Goyal S (2012) Expectation confirmation in technology use. *Inform. Systems Res.* 23(2):474–487.

Bulgurcu B, Cavusoglu H, Benbasat I (2010) Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quart.* 34(3):523–548.

Carver CS, Scheier MF (1982) Control theory: A useful conceptual framework for personality–social, clinical, and health psychology. *Psych. Bull.* 92(1):111–135.

Cenfetelli RT (2004) Inhibitors and enablers as dual factor concepts in technology usage. *J. Assoc. Inform. Systems* 5(11):472–492.

Chen M, Bargh JA (1999) Consequences of automatic evaluation: Immediate behavioral predispositions to approach or avoid the stimulus. *Personality Soc. Psych. Bull.* 25(2):215–224.

Chin WW, Marcolin BL, Newsted PR (2003) A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Inform. Systems Res.* 14(2):189–217.

Clarke NL, Furnell SM (2005) Authentication of users on mobile telephones—A survey of attitudes and practices. *Comput. Security* 24(7):519–527.

ConsumerReports (2014) Smart phone thefts rose to 3.1 million last year, consumer reports finds. (May 28), http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm.

Deterding S (2012) Gamification: Designing for motivation. *Interactions* 19(4):14–17.

Dinev T, Hu Q (2007) The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *J. Assoc. Inform. Systems* 8(7):386–408.

Ebbinghaus H (1913) *Memory: A Contribution to Experimental Psychology* (Teachers College, Columbia University, New York).

Ericsson KA, Kintsch W (1995) Long-term working memory. *Psych. Rev.* 102(2):211–245.

ESA—Entertainment Software Association (2013) 2013 sales, demographic and usage data: Essential facts about the computer and video game industry. http://www.theesa.com/facts/pdfs/ESA_EF_2013.pdf.

Fornell C, Bookstein FL (1982) Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *J. Marketing Res.* 19(4):440–452.

Herath T, Rao HR (2009) Protection motivation and deterrence: A framework for security policy compliance in organisations. *Eur. J. Inform. Systems* 18(2):106–125.

Hoffman DL, Novak TP (1996) Marketing in hypermedia computer-mediated environments: Conceptual foundations. *J. Marketing* 60(3):50–68.

Hong S, Kim J, Lee H (2008) Antecedents of user-continuance in information systems: Toward an integrative view. *J. Comput. Inform. Systems* 48(3):61–73.

Hong S, Thong JY, Tam KY (2006) Understanding continued information technology usage behavior: A comparison of three models in the context of mobile Internet. *Decision Support Systems* 42(3):1819–1834.

Huang D-L, Patrick Rau P-L, Salvendy G, Gao F, Zhou J (2011) Factors affecting perception of information security and their impacts on IT adoption and security practices. *Internat. J. Human-Comput. Stud.* 69(12):870–883.

HuffingtonPost (2012) Jenn Gibbons returns to Chicago, completing charity trip in spite of assault. (August 14), http://www.huffingtonpost.com/2012/08/14/jenn-gibbons-returns-to-c_n_1776169.html.

Ives B, Walsh KR, Schneider H (2004) The domino effect of password reuse. *Comm. ACM* 47(4):75–78.

Jakobsson M, Akavipat R (2012) Rethinking passwords to adapt to constrained keyboards. *Proc. Mobile Security Technologies, IEEE Comput. Soc. Security Privacy Workshop, San Francisco*.

Johanson M (2013) How burglars use Facebook to target vacationing homeowners. *IBT* (July 11), http://www.ibtimes.com/how-burglars-use-facebook-target-vacationing-homeowners-1341325.

Johansson J, Riley S (2005) *Protect Your Windows Network: From Perimeter to Data* (Addison-Wesley, Upper Saddle River, NJ).

Johnson K, DeLaGrange T (2012) Sans survey on mobility/BYOD security policies and practices. http://www.sans.org/reading-room/whitepapers/analyst/survey-mobility-byod-security-policies-practices-35175.

Johnston AC, Warkentin M (2010) Fear appeals and information security behaviors: An empirical study. *MIS Quart.* 34(3):549–566.

Jones BH, Heinrichs LR (2012) Do business students practice smartphone security? *J. Comput. Inform. Systems* 53(2):22–30.

Karahanna E, Straub DW, Chervany NL (1999) Information technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS Quart.* 23(2):183–213.

Karlson AK, Brush AJ, Schechter S (2009) Can I borrow your phone?: Understanding concerns when sharing mobile phones. Greenberg S, Hudson SE, Hinckley K, Morris ME, Olsen DR Jr, eds. *Proc. SIGCHI Conf. Human Factors Comput. Systems* (ACM, New York), 1647–1650.

Keisler A, Shadmehr R (2010) A shared resource between declarative memory and motor memory. *J. Neuroscience* 30(44):14817–14823.

Keith MJ, Shao B, Steinbart PJ (2007) The usability of passphrases for authentication: An empirical field study. *Internat. J. Human-Comput. Stud.* 65(1):17–28.

Keith MJ, Shao B, Steinbart PJ (2009) A behavioral analysis of passphrase design and effectiveness. *J. Assoc. Inform. Systems* 10(2):63–89.

Keller KL (1987) Memory factors in advertising: The effect of advertising retrieval cues on brand evaluations. *J. Consumer Res.* 14(3):316–333.

Kim H-W, Chan HC, Chan YP (2007) A balanced thinking—Feelings model of information systems continuance. *Internat. J. Human-Comput. Stud.* 65(6):511–525.

Lee S, Zhai S (2009) The performance of touch screen soft buttons. Greenberg S, Hudson SE, Hinckley K, Morris ME, Olsen DR Jr, eds. *Proc. SIGCHI Conf. Human Factors Comput. Systems* (ACM, New York), 309–318.

Lee Y, Larsen KR (2009) Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *Eur. J. Inform. Systems* 18(2):177–187.

Liang H, Xue Y (2009) Avoidance of information technology threats: A theoretical perspective. *MIS Quart.* 33(1):71–90.

Liang H, Xue Y (2010) Understanding security behaviors in personal computer usage: A threat avoidance perspective. *J. Assoc. Inform. Systems* 11(7):394–413.

Limayem M, Hirt SG, Cheung CM (2007) How habit limits the predictive power of intention: The case of information systems continuance. *MIS Quart.* 31(4):705–737.

MacKay B, Watters C, Duffy J (2004) Web page transformation when switching devices. Brewster S, Dunlop M, eds. *Mobile Human-Computer Interaction-MobileHCI 2004*, Lecture Notes Comput. Sci., Vol. 3160 (Springer-Verlag, Berlin Heidelberg), 228–239.

Ortiz de Guinea A, Markus ML (2009) Why break the habit of a lifetime? Rethinking the roles of intention, habit, and emotion in continuing information technology use. *MIS Quart.* 33(3):433–444.

Ortiz de Guinea A, Webster J (2013) An investigation of information systems use patterns: Technological events as triggers, the effect of time, and consequences for performance. *MIS Quart.* 37(4):1165–1188.

Park YS, Han SH, Park J, Cho Y (2008) Touch key design for target selection on a mobile phone. ter Hofte H, Mulder I, eds. *Proc. 10th Internat. Conf. Human Comput. Interaction Mobile Devices Services* (ACM, New York), 423–426.

Paul CL, Morse E, Zhang A, Choong Y-Y, Theofanos M (2011) A field study of user behavior and perceptions in smartcard authentication. Campos P, Graham N, Jorge J, Nunes N, Palanque P, Winckler M, eds. *Human-Computer Interaction—Interact 2011*, Lecture Notes Comput. Sci., Vol. 6949 (Springer-Verlag, Berlin Heidelberg), 1–17.

Payne JW (1982) Contingent decision behavior. *Psych. Bull.* 92(2):382–402.

Payne JW, Bettman JR, Johnson EJ (1993) *The Adaptive Decision Maker* (Cambridge University Press, Cambridge, UK).

Posey C, Lowry PB, Roberts TL, Ellis TS (2010) Proposing the online community self-disclosure model: The case of working professionals in France and the UK who use online communities. *Eur. J. Inform. Systems* 19(2):181–195.

Richman WL, Kiesler S, Weisband S, Drasgow F (1999) A meta-analytic study of social desirability distortion in computer-administered questionnaires, traditional questionnaires, and interviews. *J. Appl. Psych.* 84(5):754–775.

Ringle C, Wende S, Will A (2014) Smartpls 3.0. http://www.smartpls.de.

Rogers RW (1975) A protection motivation theory of fear appeals and attitude change. *J. Psych.* 91(1):93–114.

Rydell RJ, Mackie DM, Maitner AT, Claypool HM, Ryan MJ, Smith ER (2008) Arousal, processing, and risk taking: Consequences of intergroup anger. *Personality Soc. Psych. Bull.* 34(8):1141–1152.

Schneider IE, Silverberg KE, Chavez D (2011) Geocachers: Benefits sought and environmental attitudes. *Cyber J. Appl. Leisure Recreation Res.* 14(1):1–11.

Sears A, Zha Y (2003) Data entry for mobile devices using soft keyboards: Understanding the effects of keyboard size and user tasks. *Internat. J. Human-Comput. Interaction* 16(2):163–184.

Shneiderman B (1986) *Designing the User Interface-Strategies for Effective Human-Computer Interaction* (Pearson Education India, Boston).

Singh S (2012) Gamification: A strategic tool for organizational effectiveness. *Internat. J. Management* 1(1):108–113.

Smith HJ, Dinev T, Xu H (2011) Information privacy research: An interdisciplinary review. *MIS Quart.* 35(4):989–1015.

Squire LR (1986) Mechanisms of memory. *Science* 232(4758):1612–1619.

Squire LR (2004) Memory systems of the brain: A brief history and current perspective. *Neurobiology Learn. Memory* 82(3):171–177.

Tanner JF Jr, Hunt JB, Eppright DR (1991) The protection motivation model: A normative model of fear appeals. *J. Marketing* 55(3):36–45.

Taylor S, Todd PA (1995) Understanding information technology usage: A test of competing models. *Inform. Systems Res.* 6(2):144–176.

Todd P, Benbasat I (1991) An experimental investigation of the impact of computer based decision aids on decision making strategies. *Inform. Systems Res.* 2(2):87–115.

Todd P, Benbasat I (1992) The use of information in decision making: An experimental investigation of the impact of computer-based decision aids. *MIS Quart.* 16(3):373–393.

Todd P, Benbasat I (1999) Evaluating the impact of DSS, cognitive effort, and incentives on strategy selection. *Inform. Systems Res.* 10(4):356–374.

Trewin S, Swart C, Koved L, Martino J, Singh K, Ben-David S (2012) Biometric authentication on a mobile device: A study of user effort, error and task disruption. Zakon RH, ed. *Proc. 28th Annual Comput. Security Appl. Conf.* (ACM, New York), 159–168.

Tulving E, Pearlstone Z (1966) Availability versus accessibility of information in memory for words. *J. Verbal Learn. Verbal Behav.* 5(4):381–391.

Ullman MT (2004) Contributions of memory circuits to language: The declarative/procedural model. *Cognition* 92(1):231–270.

Ullman MT (2013) The declarative/procedural model of language. Pashler H, ed. *Encyclopedia of the Mind* (Sage Publications, Los Angeles), 224–226.

Vance A, Eargle D, Ouimet K, Straub D (2013) Enhancing password security through interactive fear appeals: A web-based field experiment. Sprague RH Jr, ed. *Proc. 46th Hawaii Internat. Conf. System Sciences (HICSS)* (IEEE, Los Alamitos, CA), 2988–2997.

Venkatesh V, Bala H (2008) Technology acceptance model 3 and a research agenda on interventions. *Decision Sci.* 39(2): 273–315.

Venkatesh V, Thong JYL, Xu X (2012) Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quart.* 36(1):157–178.

Venkatesh V, Brown SA, Maruping LM, Bala H (2008) Predicting different conceptualizations of system use: The competing roles of behavioral intention, facilitating conditions, and behavioral expectation. *MIS Quart.* 32(3):483–502.

Wiedenbeck S, Waters J, Birget JC, Brodskiy A, Memon N (2005) PassPoints: Design and longitudinal evaluation of a graphical password system. *Internat. J. Human-Comput. Stud.* 63(1): 102–127.

Wiener N (1948) *Cybernetics: Or Control and Communication in the Animal and the Machine* (Wiley, New York).

Woon I, Tan G-W, Low R (2005) A protection motivation theory approach to home wireless security. *Proc. Internat. Conf. Inform. Systems, Las Vegas, NV*.

Yan J, Blackwell A, Anderson R, Grant A (2004) Password memorability and security: Empirical results. *IEEE Security Privacy* 2(5):25–31.

Zviran M, Haga WJ (1999) Password security: An empirical study. *J. Management Inform. Systems* 15(4):161–185.