
# Information & Computer Security

Human-centered authentication guidelines

Jeremiah D. Still, Ashley Cain, David Schuster,

# Human-centered authentication guidelines

Jeremiah D. Still and Ashley Cain
*Department of Psychology, Old Dominion University, Norfolk, Virginia, USA, and*
David Schuster
*Department of Psychology, San Jose State University, San Jose, California, USA*



Received 21 April 2016
Revised 21 December 2016
Accepted 6 March 2017



## Abstract

**Purpose** – Despite the widespread use of authentication schemes and the rapid emergence of novel authentication schemes, a general set of domain-specific guidelines has not yet been developed. This paper aims to present and explain a list of human-centered guidelines for developing usable authentication schemes.

**Design/methodology/approach** – The guidelines stem from research findings within the fields of psychology, human–computer interaction and information/computer science.

**Findings** – Instead of viewing users as the inevitable weak point in the authentication process, this study proposes that authentication interfaces be designed to take advantage of users' natural abilities. This approach requires that one understands how interactions with authentication interfaces can be improved and what human capabilities can be exploited. A list of six guidelines that designers ought to consider when developing a new usable authentication scheme has been presented.

**Research limitations/implications** – This consolidated list of usable authentication guidelines provides system developers with immediate access to common design issues impacting usability. These guidelines ought to assist designers in producing more secure products in fewer costly development cycles.

**Originality/value** – Cybersecurity research and development has mainly focused on technical solutions to increase security. However, the greatest weakness of many systems is the user. It is argued that authentication schemes with poor usability are inherently insecure, as users will inadvertently weaken the security in their efforts to use the system. The study proposes that designers need to consider the human factors that impact end-user behavior. Development from this perspective will address the greatest weakness in most security systems by increasing end-user compliance.

**Keywords** Guidelines, Cybersecurity, Usable security, Interface design

**Paper type** General review

## Introduction

Over the past few years, cybersecurity has, unfortunately, taken center stage as cyber-attacks have become a common occurrence. On a regular basis, we learn of another cyber-attack harming individuals and businesses. For corporations, millions of dollars and reputations are at stake. For individuals, one can only guess at the far-reaching impacts of having personal information, such as fingerprints, stolen (NPR, 2015). These losses could be prevented or at least could be managed by improving our cybersecurity systems. One important security gateway for accessing services is the authentication process, which can be improved by taking a human-centered approach.

Much valuable and sensitive data (e.g. health, intellectual property and banking information) are accessible digitally. For example, we no longer have to go to a physical bank to transfer money or to cash a check. We simply download an application or go to a website. However, this level of convenience comes at a cost. Hackers worldwide are now able to access our accounts remotely. Therefore, it is essential that systems housing valuable data be able to correctly verify users' identities.

Information & Computer Security
Vol. 25 No. 4, 2017
pp. 437-453

2056-4961
DOI 10.1108/ICS-04-2016-0034

The authentication process attempts to validate a user's identity. Usually, this is achieved by asking for a username and a password known only to one user. Thus, attackers work to reveal passwords through a variety of methods, including social engineering, brute force guessing, shoulder surfing, key logging, interception and searching physical and virtual space near the target (GCHQ and CPNI, 2015). Most of the research efforts have focused on developing stronger technical defenses against these attack methods. However, users are a critical part of the security loop, so designing an authentication system that encourages appropriate behavior increases the defensive strength of the system. Users are instructed to use "strong passwords" because they are more difficult for hackers to determine. Some basic guidelines for creating strong passwords include keeping the password private and secure (do not share it or write it down), avoiding the use of common words, using longer and more complex passwords (e.g. by including numbers and symbols), using different passwords for each account and changing passwords following suspect activity. Following these "simple" guidelines demands an increased cognitive load. According to Grawemeyer and Johnson (2011), end-users reuse, share and write down passwords to overcome an effortful authentication experience. In other words, end-users are aware of many of the best practice guidelines; unfortunately, these guidelines are not usable ones. Also, some of the best practices are not necessary, if others are followed. For instance, if one takes the time to develop and remember a strong password, changing it often is not necessary.

There are many usability issues associated with conventional alphanumeric authentication. Users are forced to remember a significant number of complex passwords, which are always changing. Users are irritated by complex and changing passwords and their password selection also becomes less secure, as they are tasked with remembering many. For example, as the number of passwords increases, users are more likely to reuse the same password or some parts of an already existing password. In one study, up to 50 per cent of passwords were reused, and some were reused up to four times by the same user (Grawemeyer and Johnson, 2011). Also, when users do comply and use a unique password, they are nearly 18 times more likely to write down the password than if they had used a more familiar password (Grawemeyer and Johnson, 2011). As a result, the end-user is often the weakest link in any security system. Cybersecurity researchers are beginning to look beyond technological solutions to user-centered solutions for authentication. The hope is that, by making the interaction with authentication scheme more transparent and less effortful, users will be willing and able to comply with security measures.

A variety of methods have emerged, tokens and biometrics, for example, as attempts to replace the conventional text-based password (Matyáš and Říha, 2002). The creation of new authentication schemes has been a hot field of development for the past couple of decades (Braz and Robert, 2006). Despite the widespread use of, and the dependence on, password authentication (along with the emergence of novel authentication schemes), we still lack a general set of influencing guidelines. To meet this need, we present a list of six human-centered guidelines that designers ought to consider when developing a new authentication scheme.

Designers need to ensure that their creations follow the common core of principles such as consistency, visibility, natural mapping, constraints and feedback (Norman, 1988), given that they do not harm, in a major way, the technical security. Guidelines are an essential part of the design process. In fact, the use of expert-based evaluation techniques (i.e. heuristic evaluation and cognitive walkthrough) early in interface development can be used to detect potential issues with security systems (Chiasson *et al.*, 2006). The goal is to correct the design before it is shipped as a product, saving both time and money. In particular, expert-based evaluation techniques can be used at nearly any stage of the design process, complementing full-scale usability testing and iterative design cycles (Wickens *et al.*, 2004).

Critically, these methods depend on guidelines that are specific enough to be relevant to the developers' problem space but are general enough to accommodate innovation. They are more useful and insightful compared to the common usability principles.

Security is a seemingly competing goal with usability. Very broadly, the goals of information security can be understood through critical characteristics of information (McCumber, 1991; Cherdantseva and Hilton, 2013). Central to these characteristics are confidentiality (ensuring that only those authorized have access to the information), availability (ensuring that the mechanism for retrieving the information is operational to users) and integrity (ensuring that the information is complete and accurate). Usable security is unlikely to arise from general usability guidelines. This is because availability often conflicts with other critical characteristics of the information. General usability guidelines should result in high availability at the cost of confidentiality and integrity. If security is not considered central to the efficacy of the system, authentication impedes usability. The most usable solution, then, would be to eliminate the authentication system altogether, to provide the highest availability. Doing so, of course, would make it impossible to ensure the confidentiality or integrity of the information.

Ultimately, designers need usability guidelines that help to resolve this inherent conflict. In this article, we aim to do exactly that by providing guidelines for usable security. To ensure usable security, the guideline must lead to simultaneous improvements in usability and security. While designers may still encounter situations in which a trade-off must be made between security and usability, we argue that usability is a necessary, although not complete, condition for security. Users' workarounds for unusable technology can compromise security. Consequently, our guidelines provide a starting point for the application of usability principles designed with security in mind. For example, our guideline to inform and educate users about risk does not lower system security, even as it improves usability.

It is common to see that mature development areas have their specific human-centered guidelines. For example, augmented reality gaming (Wetzel *et al.*, 2008) and kiosk systems (Maguire, 1999) have their own design guidelines. Researchers have provided us with guidelines for developing usable personal firewalls (Johnston *et al.*, 2003) and security tool alerts (Ibrahim *et al.*, 2010). In this paper, we augment this list with our guidelines for the development of usable authentication schemes. Our guidelines emerged from a literature search focused at the intersection of authentication and human factors. Interestingly, we found that most of the relevant research had been published at the Computer – Human Interaction and SOUPS conferences. Further, it appears that communicating risk to users and developing inclusive designs have been the major themes for research across the past 10 years. According to Vidyaraman *et al.* (2008), system users are seen as the "enemy" to information technology security. Furthermore, data support the claim that users are, indeed, one of the major security weaknesses in technological systems (Verizon Data, 2013). However, users are the reason that most technological systems exist. Therefore, we must strive for a beneficial trade-off between usability and security. High failure rates and low compliance rates are reflective of the poor usability of password-based authentication schemes. Findings like these can lead authentication developers to believe that usability and security are competing views. For example, as text password complexity increases, the usability of the authentication interface rapidly decreases; as the authentication task gets easier for the user, security decreases. This issue seems to be the trend with text-based password authentication. But usable security is not an oxymoron (DeWitt and Kuljis, 2006; Still, 2016).

Instead of viewing users as the inevitable weak point in the authentication process, we propose that authentication interfaces be designed to take advantage of users' natural abilities. This approach requires that we understand both how and what: how interactions

with authentication interfaces can be improved and what human capabilities can be exploited. It has been shown that poor authentication design decisions drive users to adopt flawed approaches to security. According to Whitten and Tygar (1999), users face numerous obstacles when interacting with security systems. One of the first issues is the mismatch between the goal of the authentication scheme and the goal of the user. For instance, the user's primary goal, when interacting with an authentication scheme, is to get past the system to the services behind the point of authentication. In contrast, the primary goal of the developer of the authentication scheme is to ensure the user is who he/she claims to be.

Our goal is to consolidate the existing human-centered authentication issues into a list of immediately applicable guidelines. In doing so, we aim to inform the design of current password authentication, while guiding novel authentication schemes. This helps make expert reviews more effective within the context of authentication schemes, which ought to translate into more usable interfaces which make it easier for users to comply.

## Human-centered authentication design guidelines

### *Design to be inclusive*

Authentication interfaces are a requirement for system access for a diverse user population. Therefore, designers need to be inclusive of all populations. This includes a consideration of users' abilities, preferences, experience, social situation and technological resources (Dourish *et al.*, 2007; Meyer and Rose, 2000; Shneiderman, 2000; Vines *et al.*, 2013). To achieve accessibility, designers ought to take a universal design perspective. Considering impaired users' needs and abilities, the login process ought to be inclusive. Maintaining a secure authentication password is currently difficult enough for users, without their having to overcome extra obstacles.

This inclusivity is frequently not addressed. Ultimately, a lack of accessibility leads to poor rates for successful authentication. If users cannot successfully authenticate, companies are impacted financially. To reach a standard of ethics and to benefit companies financially, universal usability guidelines recommend that 90 per cent of users or households should be able to authenticate successfully (Shneiderman, 2000).

Older adults can experience difficulties in learning to use new technologies that are unfamiliar because of differences in their cognitive abilities, like working memory (Vines and Thompson, 2007). Many older adults tend to resist using new technology, which makes it even more important to design with the intention of ease of use for the growing older population (Vines *et al.*, 2012). Nicholson *et al.* (2013) provided an example of authentication that can be altered to increase inclusivity for older adults who typically experience declines in memory capacity after the age of 50 years. They compared younger with older participants' performances using pin authentication and face-based authentication. Although older participants did not perform as well as younger participants in all comparisons, older participants performed better for face-based authentication containing older faces (Nicholson *et al.*, 2013). These findings show that designers can alter the content of graphical authentication by using age-appropriate pictures to be more inclusive. Simple alterations in an authentication scheme can improve accessibility for the growing aging population (Vines and Thompson, 2007).

We will briefly highlight multimodal authentication schemes that were designed for those with functional impairments for whom mainstream authentication systems can be challenging (Dosono *et al.*, 2015). Kuber and Sharma (2012) described a tactile-based scheme in which users selected cues by using a mouse. The haptic feedback presented patterns in a timed sequence by raising and lowering pins on the mouse's surface. When the pins' pattern matched participants' predetermined passwords, the visually impaired could select it and could login. Further, they found that the tactile authentication scheme was appropriate for

users both with and without visual impairments. Simply reducing clutter on login pages can help visually impaired users authenticate more easily and use screen readers more easily (Dosono *et al.*, 2015). This is another example of a simple design change that can help all users, including those with visual impairments.

Fuglerud and Dale's (2011) multimodal method used a scheme with an audio one-time-password client on mobile phones. They found that two subpopulations, namely, people with visual impairments and individuals with dyslexia, were able to more easily and independently authenticate themselves when audio was added to the password client. When audio was used as a CAPTCHA, blind participants found it easy to use (Holman *et al.*, 2007) and achieved 90 per cent success rates (Lazar *et al.*, 2012). Again, these studies provide evidence that re-designs that consider multiple populations can be more inclusive.

Authentication schemes need to be designed for inclusivity, both to be non-discriminatory and to benefit businesses financially (Fuglerud and Dale, 2011). When users are frustrated or blocked when authenticating, companies lose their business. Users may not be able to access content or to complete purchases. Companies are also legally responsible for complying with accessibility policies (Olalere and Lazar, 2011). For example, if websites do not include codes that allow for people with motor or cognitive disabilities to use appropriate input and output devices, the company may be impacted financially by legal repercussions. Universal authentication can be achieved by tailoring methods to specific populations and by providing customizable modes through which authentication can occur.

*Avoid draining users' limited working memory resources*

Password complexity, a major factor in the security of a password authentication scheme, has a negative impact on how easily the password is remembered (Sasse *et al.*, 2001; Theofanos and Pfleeger, 2011). Recalling a complex password from memory is an effortful cognitive task. Designing secure but usable authentication can be challenging, as these two important aims are seemingly at odds. We refrain from demanding that designers always maximize both security and usability, which may not always be possible. Instead, we argue that authentication schemes with poor usability are inherently insecure, as users will inadvertently weaken the security in their efforts to use the authentication scheme (e.g. by attaching a sticky note with passwords onto the computer monitor). The amount of working memory that a system consumes can predict its perceived "ease of use". Working memory is described as a conscious workbench with a limited capacity (Baddeley, 1987). Operations that occur within a working memory are typically effortful and directed (Baddeley, 1992). This workbench is where we assemble, or encode, information for long-term memory storage. This effortful process is known to be serial and slow, but flexible. Critically, effortful cognitive processing is a precursor to automatic processing and to skill development (Norman and Shallice, 1986). Automatically processed procedures consume very little working memory resources, require minimal effort and can be are rendered quickly (Shiffrin and Schneider, 1977). Therefore, we encourage designers to strive for interaction consistency and to follow convention (Still and Dark, 2010, 2013). Users are consistently required to overcome arbitrary mappings between an action and a function. But, through enough consistent interaction experiences, conventional interactions can be formed and users can automatically process interfaces.

Password complexity arises while information is being encoded into long-term memory. This encoding process can be facilitated through the use of familiar and visually rich stimuli. Typically, as password complexity increases, so does security (i.e. against brute force attacks). However, making a password complex can impact how easily it can be remembered (Sasse *et al.*, 2001; Theofanos and Pfleeger, 2011). It is easier to recall a familiar name than a string of randomly selected letters. Encoding a familiar name into long-term memory is much less

effortful than encoding a random string of letters (c.f., chunking principle, Cowan, 2001). For a random string of letters, the user might have to use a mnemonic to facilitate encoding (McEvoy and Still, 2016). Using a memory strategy takes time and effort, which consumes limited working memory resources. Using a common name reduces the multidimensional search space. This reduction in possible solutions greatly decreases the computational power needed to crack a password (i.e. dictionary attack). In an attempt to overcome encoding difficulties, researchers have explored stimuli beyond alphanumeric passwords. They have found that visually rich stimuli, such as images, show superior memorability (Eljetlawi and Ithnin, 2008; Suo *et al.*, 2005). Richer stimuli provide extra sensory details that help encoding, and later recognition (c.f., picture superiority effect; Mintzer and Snodgrass, 1999). Recently, researchers have been working to overcome users' retrieval difficulties.

Recalling a complex password from memory is an effortful cognitive task. Users have to generate content from long-term memory. This is similar to completing an essay examination. A writing prompt is provided without any additional retrieval cues. This is why test-takers usually prefer completing multiple choice examinations. They provide more retrieval cues, making remembering the answer easier (Tulving and Thomson, 1973); they simply have to recognize the answer from a set containing decoys. Therefore, we recommend the use of a recognition process, rather than recall, when the passcode requires complexity. This recommendation, along with the picture superiority effect, has motivated over a decade of work within graphical authentication (Biddle *et al.*, 2012; Cain and Still, 2016).

Reducing the working memory load can be achieved in three ways. First, authentication process ought to be consistent between experiences. This guideline will allow users' cognitive systems to transfer the interaction from a conscious to an automatic process. Second, users' ability to learn new passwords should be facilitated by allowing the selection or creation of familiar passcodes that allow for rich encoding. Third, users should be helped to remember passcodes by having a recognition versus recall task provided for them.

*Inform and educate users about risk*

Interfaces do not provide concrete examples of security. Instead, they use abstract concepts and language that is full of technical jargon. The mismatch between user and interface goals and the failure of interfaces to communicate security goals to the users can contribute to the frequency with which users break security policies or circumnavigate them altogether (Beautement *et al.*, 2016). In many cases, users are not intentionally non-compliant. They need usable interfaces that clearly communicate security needs, states and risks (Kuo *et al.*, 2009; Smith, 2003; Stephano and Groth, 2006).

For a system to be secure, we need users to be situationally aware of the risk that might result from their actions. Designers must consider what kind of information is being protected (e.g. sensitive, confidential, private or public) and should make end-users aware of the associated risk (Renaud, 2007). They should follow a classification scheme of low, medium, high and very high risk when communicating with end-users. Effectively communicating risk to users is worth the development costs. The more that a user understands a threat and perceives a threat as severe, the more likely they will behave protectively (Forget *et al.*, 2016; Kang *et al.*, 2015; Woon *et al.*, 2005), such as installing antivirus software (Lee and Larsen, 2009) or selecting a stronger passcode (Egelman *et al.*, 2013; Ur *et al.*, 2016).

Communicating risk to users both helps them to understand why security may be more strenuous and encourages the adoption of new security policies. Zhang and McDowell (2009, p. 13) explain:

> The security level of the password mechanism largely depends on users' willingness to make efforts to behave in accordance with strong password policies. However, they have to be persuaded to do so.

End-user behaviors can either bolster or undermine security, depending on their appreciation for risk (Zhang and McDowell, 2009). Grawemeyer and Johnson (2011) observed that users tend to use more complex alphanumeric passwords for services that are perceived to have more sensitive information. When immediate feedback is provided about the strength of a new password, users create stronger passwords for accounts that are perceived as important (Egelman *et al.*, 2013; Shay *et al.*, 2015). Therefore, when there is risk associated with information, users' perceptions of this risk can be productive for security. Security is bolstered when users both understand that there are risks associated with information and understand the causal attributes of the risk (Beris *et al.*, 2015).

End-users typically perceive themselves to be at less risk for vulnerabilities than average users (Zhang and McDowell, 2009). There is a false belief that although cyber-attacks are common, a user will not become a target. Because of this misperception, end-users are not motivated to use strong security because of the perceived lack of benefit. For example, passwords are usually re-used between 1.7 and 3.4 websites (Wash *et al.*, 2016), and a third of participants reported sharing their email passwords with friends or loved ones (Kaye, 2011). Users frequently do not understand appropriate security measures for email, and about 30 per cent of accounts have been hijacked (Shay *et al.*, 2014). A majority of passwords for an e-commerce website were crackable in less than 4 h and one-third of passwords were crackable in less than 1 min (Cazier and Medlin, 2006). Lock screens for mobile phones are considered unnecessary 24.1 per cent of the time, and users underestimate the threat of over-the-shoulder attacks (Harbach *et al.*, 2014). Motivation toward security can be increased through accurate conceptions about costs, or risks and benefits (Fagan and Khan, 2016).

The risk that an attack will occur (or the opportunity that an attacker can complete an attack) is defined as (Renaud, 2007, p. 17):

$$\text{Opportunity} = \frac{f(\text{Guessability; Observability; Recordability; Analyzability})}{\text{Resistibility}}$$

Communicating with end-users and educating them about better habits and practices can help diminish the risk that comes from their behaviors. They need to be aware of the risk of recordability that comes from writing down passwords or telling someone a password (Renaud, 2007). With the proliferation of alphanumeric passwords, many users record passwords to aid memory. There is a risk of observability that comes from shoulder-surfing (Renaud, 2007). For example, users' mobile phone passwords may be compromised by onlookers in public places. End-users should be aware of guessability (the strength of an authentication passcode). Many users tend toward simple passwords that are easier to remember but which are often easier to guess. Analyzability is a risk that comes from mechanisms of software (Renaud, 2007). An awareness of software vulnerabilities can help users tailor their behaviors appropriately. The opportunity for risk factors to become realized in an attack is constrained by a system's resistibility (Renaud, 2007). For example, a system may be resistant to attack if it limits the number of inaccurate login attempts or locks the user out of the system after a time interval.

When designing for security, it is important to keep the role of the end-user in mind. They can ultimately decide to undermine or bypass the security measures if they find them inconvenient or unnecessary. They need to be informed and educated about the level of risk inherent in the protected information and the risk that comes from their behaviors. Ideally, we recommend that these inappropriate behaviors be designed out. However, often a major redesign is not possible, given development constraints. However, risk can be communicated through the system (e.g. warnings and training). Training can be personalized, to increase

motivation toward security. Users can be educated about their personal privacy and safety and their personal impact. For example, Take This Lollipop is a website that shows an illustrated, personalized example to communicate to users that the information they post on Facebook can be used by attackers to target them (Take This Lollipop, 2017). Warnings for application downloads on mobile phones can provide personalized examples of information that would become vulnerable after the download, such as the user's photos that could be accessed by attackers (Harbach *et al.*, 2014). Information is more persuasive and more likely to elicit agreement when a user's personal involvement is communicated (Petty and Cacioppo, 1984). An understanding of their actual vulnerability and consequences of compromised information can motivate users to be more conscious of their actions.

*Eliminate jargon by considering users' mental models*

Interfaces often use jargon, which can create a distance between an interface's representation and the user's mental model. This distance can create gulfs that are perceived to be too wide to cross (Hutchins *et al.*, 1986). This might implicitly encourage users to disengage, misunderstand and lose motivation to learn.

Users' understandings of a complex system, such as a website, can be conceptualized using mental models. They are "the mechanisms whereby humans can generate descriptions of system purpose and form, explanations of system functioning and observed system states, and predictions of future states" (Rouse and Morris, 1986, p. 351). Mental models are the users' understandings of the pieces and how the pieces fit together. While reducing jargon is an important user-centered guideline (Assal *et al.*, 2015; Garfinkel, 2015), the use of jargon presents specific problems in a security context, as it further disempowers users to participate in their own security.

*Mental models and transparency.* Mental models can be described along two dimensions: accuracy and complexity. A mental model of a bicycle that includes wheels, a frame and pedals is accurate but is not very complex. Both the accuracy and the complexity of mental models are hallmarks of high-performing experts in a domain. Consequently, Web developers can be expected to have an accurate and complex mental model of their systems. However, users' mental models are often poor, especially with websites that provide limited transparency of their backend processing (Muramatsu and Pratt, 2001). Transparency can be defined as a quality of the authentication scheme; when services explain what is happening behind the scenes, so that users understand why the service is behaving in a particular way, the service is transparent. Transparency can also be defined as a user-centered outcome. Users can be queried to see if they understand why a service behaved in a particular way. For example, an authentication scheme should be transparent so that if a user is not authenticated, the user understands why. Without transparency, users' progress toward their goals are impeded.

Users hold many mental models in the course of their work. A Web developer may hold mental models of the primary programming language, database schema, page links, user preferences and more. Users may hold mental models of the working of the internet, the navigational structure of a website and the relationship among products when shopping. Of these mental models, nontechnical users are likely to have simple and potentially inaccurate mental models of the technological components of a website, including the authentication scheme. Developers of authentication are likely to have the most accurate and complex mental models of these aspects of a website. The result is a gap between user and developer understanding, which can and should be remedied through usability evaluation methods.

Authentication needs to be clear and usable for users with poor and inaccurate mental models. Poor mental models prevent users from representing the authentication process internally, and thus, they are more likely to become confused or lost in the process.

Inaccurate mental models are similarly harmful to user interactions. Their use may cause incorrect predictions about future states in the authentication process. Also, users may engage in unexpected behavior that can impede their progress through the authentication scheme. These issues have been documented in a usability evaluation of the PGP 5.0 encryption process (Whitten and Tygar, 1999). To mention an example specific to authentication: if a user does not understand how two-factor authentication works in an authentication scheme, the user might attempt to skip this step or might provide a verification phone number that they do not have access to. Thus, the hypothetical user would be locked out of the service. Less experienced users with less accurate mental models have been observed to ignore or uninstall firewalls that block risky connections (Raja *et al.*, 2010).

Designers can anticipate these issues and can design for users with poor or inaccurate mental models, in part, by eliminating jargon. Jargon can be defined as "special words or expressions that are used by a particular profession or group and are difficult for others to understand" (Jargon, 2016). However, authentication scheme development often occurs in an environment with multiple stakeholders. Thus, jargon is relative. Developers should identify jargon relative to their user population through the human-centered design process. Remember that users do not understand how the authentication scheme works. They will try to put the pieces together as they build understanding. It is important, then, that the authentication scheme can be used even with an inaccurate mental model. Observations of users misconfiguring or defeating security features are hints at usability issues in the design. Users must be empowered to make decisions that improve security, even if they have a poor understanding of security fundamentals, which is often the case (Furnell, 2005).

Jargon is of no benefit to users in authentication, and it may even hinder usability in unanticipated ways by being incompatible with users' mental models. This issue furthers the gulf between what designers anticipate that users will do and the actual behavior of the end users (Hutchins *et al.*, 1986). Consequently, jargon simultaneously impedes user satisfaction and performance, even as it lowers security. However, designers must focus on the particularly harmful effect of jargon in the authentication process, which can interact with users' limited understanding. For this reason, we have included the elimination of jargon as a design guideline. An innovative authentication scheme that must teach the user new terms is unlikely to reflect usable security.

*Make appropriate actions apparent*

Too often, the authentication process takes our attention away from our primary task. To minimize this disruption, the interface interactions necessary for authentication must be apparent. Users are motivated by and should focus on their primary task to meet their goal. For example, purchasing the best-priced bike tire might be their goal. Specifically, then, a user has a primary task of navigating a website to find the lowest cost "700 × 23 mm" road tire. A secondary task is becoming a member of the website to complete the purchase. If other sites offer a similarly priced bike tire and joining is perceived as difficult, they will complete the transaction elsewhere. Therefore, successful designers focus on supporting users' primary tasks and minimizing secondary task distractions. Recognizing and supporting users' motivation can often be difficult when attempting to balance an array of other technical requirements, including security. We argue that the best approach is to assume that users are motivated only by their primary goals and not by any reward or intrinsic value in the authentication process. Consequently, the impact of usability problems in authentication systems is magnified, relative to those affecting a user's primary task.

Authentication is always a secondary task for users. They do not authenticate for itself. Authentication is an interruption in the process of deciding and executing an action toward

meeting a goal. Consequently, bad authentication schemes may compete for working memory resources to such an extent that users' limited working memory pools are depleted. In such a case, users' goals are impeded, producing a poor-quality user experience. Many loyal users may attempt to overcome the poor experience by disregarding or circumventing authentication policies.

Multitasking requires users to constantly switch limited cognitive resources among the ongoing tasks needed to meet a goal. Therefore, designers need to consider the factors that impact the ability of users to multitask effectively. According to Wickens' (2008) multiple resource theory, working memory is available to us as a finite resource that can be depleted. We do have several working memory pools, but tasks can compete for resources within a single pool. For example, two tasks that are both highly verbal, such as a reading a book and holding a conversation, are likely to compete for limited resources more than two tasks drawing from different pools (e.g. holding a conversation and riding a bicycle). Knowing this, designers need to consider the type of resources being consumed by the primary task and avoid drawing from the same pool for authentication.

Consequently, usable authentication schemes must avoid distracting from the primary task. To achieve this, authentication schemes need to be both apparent and intuitive. Apparent means that the user's attention needs to be quickly drawn to critical authentication elements. Authentication login elements should be salient enough to facilitate users' ability to find where to start the process. To help minimize distraction, authentication interfaces ought to limit physical and cognitive effort. In this way, they must be intuitive. Systems should capitalize on users' previous experience, to limit the number of attentional demands associated with resolving novel interaction ambiguity.

Often, developers want to encourage users in their primary task (e.g. completing a shopping transaction), so they should minimize the effort required to authenticate as much as possible. As with all guidelines presented here, minimizing distraction and limited cognitive resource consumption needs to be considered, not just at login but also during other authentication operations, such as passcode changing, initial enrollment and account closure.

*Provide users quick access*

Clearly, logging into a system is not the primary task. Further, authentication is often required numerous times throughout the day, and such a high-frequency task needs to be brief. Users want to quickly get beyond authentication. Thus, the temporal dimension of authentication impacts the perceived quality. This is similar to users setting different download expectations times for text and graphic Web pages (Shneiderman and Plaisant, 2010). Authentication schemes that are perceived to slow users' progress toward meeting a goal will cause frustration. Time is a valuable resource for users.

However, Widenbeck *et al.* (2006) claim that users consider the "fun factor" when determining the acceptability of an authentication scheme. We simply disagree. They created the Convex Hull Click Scheme. Their approach did not require users to select their pass icons; rather, users mentally identified their locations. Users authenticated by choosing decoy icons within their pass icons' boundaries across multiple rounds. On average, it took users 72 seconds to log in. We might rate the authentication process as fun for the first dozen logins. However, we predict that the fun factor would quickly fade. We believe that this drop in "fun factor" would result from the authentication's becoming the primary task and its taking the user longer to log in than expected.

The conventional approach (for instance, alphanumeric-based authentication) more matches our expectations. According to Braz and Robert (2006), the typical password login process takes between 7 and 20 s. Further, personal identification number (PIN) take about 5 to 10 s to

enter. Researchers developing SwiPIN, a novel PIN authentication scheme, which offers greater resistance to over-the-shoulder attacks, were able to maintain the perception of a fast login by only requiring an additional 2 s (von Zezschwitz *et al.*, 2015). It appears that biometrics (i.e. fingerprint, hand recognition, voice) are the fastest method of authentication, occurring in less than 5 s (Braz and Robert, 2006). Therefore, it appears that an authentication process that requires more than 20 s will be experienced as inferior. It is possible to design graphical authentication schemes that provide quick access. According to Werner *et al.* (2016), well-designed graphical passcodes can reflect rapid entry times only slightly more slowly than traditional keyboard-based schemes. It might be the case that the additional hassle is worth it, regarding security. In these cases, we recommend that extra attention be taken to justify the longer login processes to users.

## Conclusion

The greatest weakness of many systems is the user (Verizon Data, 2013). According to one of the most infamous hackers, Kevin Mitnick:

> The human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption, and secure access devices, and it is money wasted because none of these measures address the weakest link in the security chain (Poulsen, 2000).

We need to develop cybersecurity systems that consider user strengths and design-out their weaknesses. This perspective will address the greatest weakness in any security system by increasing user compliance (Sasse *et al.*, 2001). A developer can create a technically outstanding authentication scheme. However, if users attach a sticky note to the monitor with the passcode written on it, the technical aspects of the security design are rendered worthless. Even the best programming cannot prevent thieves from accessing the valuable information if the passcode can be viewed.

When considering the effectiveness of authentication schemes, designers need to actively consider user diversity. Human-centered designers must attempt to create authentication schemes that can be used by the broadest possible population, regardless of background or abilities. If they do not, the implementation has a high probability of failure. For example, in July 2015, the US Social Security Administration briefly required all Americans to have a cellular phone number to manage their benefits using the new two-factor authentication scheme. Only a month later, this authentication scheme was revoked due to both security and inclusiveness concerns (e.g. elderly users not having SMS service). Designers need to identify diversity in their user populations, whether that diversity be in cognitive, perceptual or physical ability, or in accessibility to resources. This knowledge will help them design for the wide range of users which is often a requirement for authentication systems.

It is human nature to forget passcodes or to make mistakes, but we can minimize the number of working memory resources needed to retrieve a forgotten passcode by providing useful memory cues. Too often, current authentication schemes do not remind users of their specific passcode requirements following a failed login attempt. Further, if a passcode was recently changed, it should be noted specifically when that update occurred. This feedback helps users recreate the passcode learning context, which supports easier memory retrieval. Additionally, short-term password reset intervals should not be set (GCHQ and CPNI, 2015). Asking users to learn a new password increases the scheme's working memory burden. The impact of design decisions on working memory load needs to be considered. Especially, attention must be paid to design consistency and to the current design conventions that users are using to resolve interaction ambiguity. Situating interactions reveals possible redesign opportunities (like facilitating memory retrieval) and unavoidable threats.

Ultimately, individual passwords will be stolen or accidentally shared publicity. It is critically important that we remind users to always use a unique passcode and to personalize their risk. We know that many users reuse passcodes and currently lack the complete understanding of the associated dangers of these practices. Thus, designers need to leverage users' existing knowledge of risk or communicate the risk to the user. This will be a difficult design issue as illustrated within the current literature (e.g. poor mental models, lack of motivation). This carelessness or lack of understanding on the part of the user means that passwords will always need to be updatable. Further, given that passcodes are being targeted, we ought to separate sensitive information from their password. According to Matyáš and Říha (2002), for instance, biometrics may reveal the likelihood of medical conditions. To prevent privacy violations, authentication schemes should not contain information beyond what is needed for validating an identity. This will be particularly challenging for biometric approaches. Clearly, biometrics are fast, will not be forgotten and typically are easy to use. Biometrics satisfy our usability guidelines. But, some biometric authentication schemes do not ask for secret, but for public, information (e.g. selfie video). Also, they introduce new technical difficulties, like verifying whether the data are the "real thing" (e.g. a live face). It is important to remember that any novel authentication scheme will always be targeted, so we must expect failure and plan for recovery.

Although some users are not motivated to prioritize security, many tech-savvy users are attempting to develop more accurate mental models, but the lack of standardization across, and often within, classes of products leads to confusion. Password requirements can be unclear. For example, what is considered a special character and what "common" words cannot be used? Usability testing can be used to detect and verify this poor communication is resolved. Eliminating jargon is the starting step toward better learnability. For example, it is difficult to quickly learn the difference between "two-step verification" and "two-step authentication". This ambiguity not only harms the rapid development of the correct mental models it provides but it also presents another way for hackers to take advantage of the human element.

Designers need to consider users' workflow, context and available tools to enhance security and perceived usability. For instance, forcing users to type passwords on mobile devices is not going to provide users with quick access. Therefore, authentication schemes ought to allow copy-and-paste, along with password manager support, especially in mobile use cases. Also, make the appropriate authentication processes apparent. For example, designers can increase the authentication elements' visual saliency and place it in a conventional location. An interface's authentication access element is often the starting point for users. This will help users quickly navigate the interface to get to the login. However, usable security is not only about maximizing usability.

We argue that data security and data access often trade-off in authentication schemes. In resolving this tradeoff, designers must consider the data security needs of all stakeholders, as well as the need for data access. For example, customers will not accept technical security obstacles, which could cost business, but military personnel working with classified data will tolerate additional authentication steps. However, sacrifices in data access to ensure security are no excuse for poor usability, which could impact user acceptance (Porter *et al.*, 2012). Our guidelines apply both when data security and data access needs are balanced and when one of the needs takes priority.

We hope that these human-centered guidelines will help designers to develop more usable authentication schemes and to improve the security of existing ones. This could be achieved by facilitating productive authentication heuristic evaluations and by designing a usable authentication scheme that naturally encourages appropriate end-user behaviors.

## References

Assal, H., Hurtado, S., Imran, A. and Chiasson, S. (2015), "What's the deal with privacy apps? A comprehensive exploration of user perception and usability", *Proceedings of the 14th International Conference on Mobile and Ubiquitous Multimedia*, *Linz*, pp. 25-36.

Baddeley, A. (1987), "Oxford psychology series, No. 11. Working memory", *Journal of Neurology, Neurosurgery, & Psychiatry*, Vol. 50 No. 5, pp. 654-655.

Baddeley, A. (1992), "Working memory", *Science*, Vol. 255 No. 504, pp. 556-559.

Beautement, A., Becker, I., Parkin, S., Krol, K. and Sasse, M.A. (2016), "Productive security: a scalable methodology for analyzing employee security behaviors", *Symposium on Usable Privacy and Security (SOUPS)*, Denver, CO, 22-24 June.

Beris, O., Beautement, A. and Sasse, M.A. (2015), "Employee rule breakers, excuse makers and security champions: mapping the risk perceptions and emotions that drive security behaviors", *Proceedings of the 2015 New Security Paradigms Workshop*, *ACM*, *Twente*, September, pp. 73-84.

Biddle, R., Chiasson, S. and Van Oorschot, P.C. (2012), "Graphical passwords: learning from the first twelve years", *ACM Computing Surveys*, Vol. 44 No. 4, pp. 1-41.

Braz, C. and Robert, J.M. (2006), "Security and usability: the case of the user authentication methods", *Proceedings of the 18th International Conference of the Association Francophone Interaction Homme-Machine, ACM*, *New York, NY*, pp. 199-203.

Cain, A.A. and Still, J.D. (2016), "A rapid serial visual presentation method for graphical-authentication", in Nicholson, D. (Ed.), *Advances in Human Factors Cybersecurity*, Springer, Walt Disney World, FL, pp. 3-12.

Cazier, J.A. and Medlin, B.D. (2006), "Password security: an empirical investigation into ecommerce passwords and their crack times", *Information Systems Security*, Vol. 15 No. 6, pp. 45-55.

Cherdantseva, Y. and Hilton, J. (2013), "A reference model of information assurance & security", *Proceedings of the 8th International Conference on Availability, Reliability and Security*, *Guimaraes*.

Chiasson, S., van Oorschot, P.C. and Biddle, R. (2006), "A usability study and critique of two password managers", *Usenix Security*, Vol. 6, pp. 1-16.

Cowan, N. (2001), "Metatheory of storage capacity limits", *Behavioral and Brain Sciences*, Vol. 24 No. 1, pp. 1-154.

DeWitt, A.J. and Kuljis, J. (2006), "Aligning usability and security: a usability study of Polaris", *Proceedings of the Second Symposium on Usable Privacy and Security*, *ACM*, *Pittsburgh, PN*, pp. 1-7.

Dosono, B., Hayes, J. and Wang, Y. (2015), "I'm stuck!": a Contextual inquiry of people with visual impairments in authentication", *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015*, pp. 151-168.

Dourish, P., Anderson, K. and Nafus, D. (2007), "Cultural mobilities: diversity and agency in urban computing", *FIP Conference on Human-Computer Interaction, Springer*, *Verlag Berlin, Heidelberg*, (September), pp. 100-113.

Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K. and Herley, C. (2013), "Does my password go up to eleven? The impact of password meters on password selection", *Proceedings of The SIGCHI Conference on Human Factors in Computing Systems*, *ACM*, *Paris*, April, pp. 2379-2388.

Eljetlawi, A.M. and Ithnin, N. (2008), "Graphical password: comprehensive study of the usability features of the recognition base graphical password methods", *Convergence and Hybrid Information Technology, 2008. ICCIT'08. Third International Conference IEEE*, *Busan*, Vol. 2, pp. 1137-1143.

Fagan, M. and Khan, M.M.H. (2016), "Why do they do what they do? A study of what motivates users to (not) follow computer security advice", *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*.

Forget, A., Pearman, S., Thomas, J., Acquisti, A., Christin, N., Cranor, L.F., Egelman, S., Harbach, M. and Telang, R. (2016), "Do or do not, there is no try: user engagement may not improve security outcomes", *Symposium on Usable Privacy and Security (SOUPS)*, June.

Fuglerud, K.S. and Dale, Ø. (2011), "Secure and inclusive authentication with a talking mobile one-time-password client", *IEEE Security & Privacy Magazine*, Vol. 9 No. 2, pp. 27-34.

Furnell, S. (2005), "Why users cannot use security", *Computers & Security*, Vol. 24 No. 4, pp. 274-279.

Garfinkel, S. (2015), "De-identification of personally identifiable information", National Institute of Science and Technology, Technical Report NIST IR 8053, available at: http://dx.doi.org/10.6028/NIST.IR.8053

GCHQ and CPNI (2015), "Simplifying your approach: password guidance", available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf

Grawemeyer, B. and Johnson, H. (2011), "Using and managing multiple passwords: a week to a view", *Interacting with Computers*, Vol. 23 No. 3, pp. 256-267.

Harbach, M., Hettig, M., Weber, S. and Smith, M. (2014), "Using personal examples to improve risk communication for security & privacy decisions", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, Ottawa*, April, pp. 2647-2656.

Harbach, M., von Zezschwitz, E., Fichtner, A., De Luca, A. and Smith, M. (2014), "It's a hard lock life: a field study of smartphone (un) locking behavior and risk perception", *Symposium On Usable Privacy and Security (SOUPS 2014)*, pp. 213-230.

Holman, J., Lazar, J., Feng, J.H. and D'Arcy, J. (2007), "Developing usable CAPTCHAs for blind users", *Proceedings of the 9th International ACM SIGACCESS Conference on Computers and Accessibility, ACM, Tempe, AZ,* October, pp. 245-246.

Hutchins, E.L., Hollan, J.D. and Norman, D.A. (1986), "Cognitive engineering", *User Centered System Design: New Perpectives on Human-Computer Interaction*, Lawrence Erlbaum Associates, pp. 87-124.

Ibrahim, T., Furnell, S., Papadaki, M. and Clarke, N.L. (2010), "Assessing the usability of end-user security software", *Trust, Privacy and Security in Digital Business*, pp. 177-189.

Jargon (2016), "Oxford English dictionary online", (2nd ed.), available at: https://en.oxforddictionaries.com/definition/jargon

Johnston, J., Eloff, J.H. and Labuschagne, L. (2003), "Security and human computer interfaces", *Computers & Security*, Vol. 22 No. 8, pp. 675-684.

Kang, R., Dabbish, L., Fruchter, N. and Kiesler, S. (2015), "My data just goes everywhere: user mental models of the internet and implications for privacy and security", *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pp. 39-52.

Kaye, J.J. (2011), "Self-reported password sharing strategies", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, Vancouver, BC*, May, pp. 2619-2622.

Kuber, R. and Sharma, S. (2012), "Developing an extension to an existing tactile authentication mechanism to support non-visual interaction", *Proceedings of the Conference on Human-Computer Interaction, Birmingham*, pp. 190-198.

Kuo, C., Perrig, A. and Walker, J. (2009), "Security configuration for nonexperts: a case study in wireless network configuration", *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*, IGI Global, pp. 179-195.

Lazar, J., Feng, J., Brooks, T., Melamed, G., Wentz, B., Holman, J., Olalere, A. and Ekedebe, N. (2012), "The SoundsRight CAPTCHA: an improved approach to audio human interaction proofs for blind users", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, Austin, TX*, May, pp. 2267-2276.

Lee, Y. and Larsen, K.R. (2009), "Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 177-187.

McCumber, J. (1991), "Information systems security: a comprehensive model", *Proceedings of the 14th National Computer Security Conference, Washington, DC*, pp. 1-6.

McEvoy, P. and Still, J.D. (2016), "Contextualizing mnemonic phrase passwords", in Nicholson, D. (Ed.), *Advances in Human Factors Cybersecurity*, Springer, Walt Disney World, FL, pp. 295-304.

Maguire, M.C. (1999), "A review of user-interface design guidelines for public information kiosk systems", *International Journal of Human-Computer Studies*, Vol. 50 No. 3, pp. 263-286.

Matyáš, V. and Říha, Z. (2002), "Biometric authentication—security and usability", *Advanced Communications and Multimedia Security*, Springer, pp. 227-239.

Meyer, A. and Rose, D.H. (2000), "Universal design for individual differences", *Educational Leadership*, Vol. 58 No. 3, pp. 39-43.

Mintzer, M.Z. and Snodgrass, J.G. (1999), "The picture superiority effect: support for the distinctiveness model", *The American Journal of Psychology*, Vol. 112 No. 1, pp. 113-146.

Muramatsu, J. and Pratt, W. (2001), "Transparent queries: investigation users' mental models of search engines", *Proceedings of the 24th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval, ACM, New Orleans, LA*, pp. 217-224.

Nicholson, J., Coventry, L. and Briggs, P. (2013), "Age-related performance issues for PIN and face-based authentication systems", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, Paris*, pp. 323-332.

Norman, D.A. (1988), *The Psychology of Everyday Things*, Basic Books.

Norman, D.A. and Shallice, T. (1986), *Attention to Action*, Springer, pp. 1-18.

NPR (2015), "Biometrics may ditch the password, but not the hackers", available at: www.npr.org/sections/alltechconsidered/2015/04/23/401466507/biometrics-may-ditch-the-password-but-not-the-hackers (accessed 4 April 2016).

Olalere, A. and Lazar, J. (2011), "Accessibility of US federal government home pages: Section 508 compliance and site accessibility statements", *Government Information Quarterly*, Vol. 28 No. 3, pp. 303-309.

Petty, R.E. and Cacioppo, J.T. (1984), "The effects of involvement on responses to argument quantity and quality: central and peripheral routes to persuasion", *Journal of Personality and Social Psychology*, Vol. 46 No. 1, pp. 69-81.

Porter, C., Sasse, M.A. and Letier, E. (2012), "Designing acceptable user registration processes for e-services", *Proceedings of 26th Annual BCS Conference on Human Computer Interaction: Designing Interactive Secure Systems, Birmingham, AL*, pp. 1-4.

Poulsen, K. (2000), "Mitnick to lawmakers: people, phones, and weakest links", available at: www.politechbot.com/p-00969.html (accessed 4 April 2016).

Raja, F., Hawkey, K., Jaferian, P., Beznosov, K. and Booth, K.S. (2010), "It's too complicated, so I turned it off! Expectations, perceptions, and misconceptions of personal firewalls", *Proceedings of the 3rd ACM Workshop on Assurable and Usable Security Configuration, ACM, Chicago, IL*, pp. 53-62.

Renaud, K. (2007), "A process for supporting risk-aware web authentication mechanism choice", *Reliability Engineering & System Safety*, Vol. 92 No. 9, pp. 1204-1217.

Rouse, W.B. and Morris, N.M. (1986), "On looking into the black box: prospects and limits in the search for mental models", *Psychological Bulletin*, Vol. 100 No. 3, pp. 349-431.

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

Shay, R., Bauer, L., Christin, N., Cranor, L.F., Forget, A., Komanduri, S., Mazurek, M., Melicher, W., Segreti, S. and Ur, B. (2015), "A spoonful of sugar? The impact of guidance and feedback on password-creation behavior", *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, ACM, Seoul*, April, pp. 2903-2912.

Shay, R., Ion, I., Reeder, R.W. and Consolvo, S. (2014), "My religious aunt asked why i was trying to sell her Viagra: experiences with account hijacking", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, Toronto*, April, pp. 2657-2666.

Shiffrin, R.M. and Schneider, W. (1977), "Controlled and automatic human information processing: II: perceptual learning, automatic attending and a general theory", *Psychological Review*, Vol. 84 No. 2, pp. 127-190.

Shneiderman, B. (2000), "Universal usability", *Communications of the ACM*, Vol. 43 No. 5, pp. 84-91.

Shneiderman, B. and Plaisant, C. (2010), *Designing the User Interface: Strategies for Effective Human-Computer Interaction*, Addison-Wesley, Reading, MA.

Smith, S.W. (2003), "Humans in the loop: human-computer interaction and security", *IEEE Security & Privacy Magazine*, Vol. 1 No. 3, pp. 75-79.

Stephano, A.L. and Groth, D.P. (2006), "Useable security: interface design strategies for improving security", *Proceedings of the 3rd International Workshop on Visualization for Computer Security, ACM, Alexandria*, pp. 109-116.

Still, J.D. (2016), "Cybersecurity needs you!", *ACM Interactions*, Vol. 23 No. 3, pp. 54-58.

Still, J.D. and Dark, V.J. (2010), "Examining working memory load and congruency effects on affordances and conventions", *International Journal of Human-Computer Studies*, Vol. 68 No. 9, pp. 561-571.

Still, J.D. and Dark, V.J. (2013), "Cognitively describing and designing affordances", *Design Studies*, Vol. 34 No. 3, pp. 285-301.

Suo, X., Zhu, Y. and Owen, G.S. (2005), "Graphical passwords: a survey", *21st Annual Conference on Computer Security Applications, IEEE*, Washington, DC, pp. 1-10.

Take This Lollipop (2017), available at: www.takethislollipop.com/ (accessed 12 April 2016).

Theofanos, M.F. and Pfleeger, S.L. (2011), "Guest editors' introduction: shouldn't all security be usable?", *IEEE Security & Privacy Magazine*, Vol. 9 No. 2, pp. 12-17.

Tulving, E. and Thomson, D.M. (1973), "Encoding specificity and retrieval processes in episodic memory", *Psychological Review*, Vol. 80 No. 5, pp. 352-373.

Ur, B., Bees, J., Segreti, S.M., Bauer, L., Christin, N., Cranor, L.F. and Deepak, A. (2016), "Do users' perceptions of password security match reality?" *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI), San Jose, CA*, May.

Verizon Data (2013), "Data breach investigation report", available at: www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf (accessed 14 April 2016).

Vidyaraman, S., Chandrasekaran, M. and Upadhyaya, S. (2008), "Position: the user is the enemy", *Proceedings of the 2007 Workshop on New Security Paradigms, North Conway, NH*, pp. 75-80.

Vines, J., Blythe, M., Dunphy, P., Vlachokyriakos, V., Teece, I., Monk, A. and Olivier, P. (2012), "Cheque mates: participatory design of digital payments with eighty somethings", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, Austin, TX*, May, pp. 1189-1198.

Vines, J., McNaney, R., Clarke, R., Lindsay, S., McCarthy, J., Howard, S. and Wallace, J. (2013), "Designing for-and with-vulnerable people", *CHI'13 Extended Abstracts on Human Factors in Computing Systems*, ACM, Paris, April, pp. 3231-3234.

Vines, J. and Thompson, S. (2007), "Aging futures: towards an inclusive cognitive interaction design", *The International Conference for Inclusive Design, The Royal College of Art, Kensington Gore, London*, 2-4 April, ISBN 1-905000-34-0.

Von Zezschwitz, E., De Luca, A., Brunkow, B. and Hussmann, H. (2015), "SwiPIN – Fast and secure PIN-entry on smartphones", *Proceedings of the Computer-Human Interaction (CHI) Conference, ACM, San Jose, CA*, pp. 1403-1406.

Wash, R., Rader, E., Berman, R. and Wellmer, Z. (2016), "Understanding password choices: how frequently entered passwords are re-used across websites", *Symposium on Usable Privacy and Security (SOUPS)*, Santa Clara, CA, June.

Werner, S., Hauck, C. and Masingale, M. (2016), "Password entry times for recognition-based graphical passwords", *Proceedings of the Human Factors and Ergonomics Society Conference*, *Washington, DC*, pp. 754-758.

Wetzel, R., McCall, R., Braun, A.K. and Broll, W. (2008), "Guidelines for designing augmented reality games", *Proceedings of the 2008 Conference on Future Play: Research, Play, Share*, *ACM*, *Toronto, Ontario*, pp. 173-180.

Whitten, A. and Tygar, J.D. (1999), "Why Johnny can't encrypt: a usability evaluation of PGP 5.0", *Proceedings of the 8th conference on USENIX Security Symposium*, *Washington, DC*, 23-26 August, pp. 1-15.

Wickens, C.D. (2008), "Multiple resources and mental workload", *Human Factors: The Journal of the Human Factors and Ergonomics Society*, Vol. 50 No. 3, pp. 449-455.

Wickens, C.D., Alexander, A.L., Horrey, W.J., Nunes, A. and Hardy, T.J. (2004), "Traffic and flight guidance depiction on a synthetic vision system display: the effects of clutter on performance and visual attention allocation", *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 48 No. 1, pp. 218-222.

Widenbeck, S., Waters, J., Sobrado, L. and Birget, J. (2006), "Design and evaluation of a shoulder-surfing resistant graphical password scheme", *AVI'06, Proceedings of the Working Conference on Advanced Visual Interfaces*, *Venice*, pp. 177-184.

Woon, I., Tan, G.W. and Low, R. (2005), "A protection motivation theory approach to home wireless security", *ICIS 2005 Proceedings*, *Fort Worth, TX*, pp. 367-380.

Zhang, L. and McDowell, W.C. (2009), "Am I really at risk? Determinants of online users' intentions to use strong passwords", *Journal of Internet Commerce*, Vol. 8 Nos 3/4, pp. 180-197.

## Further reading

Belk, M., Fidas, C., Germanakos, P. and Samaras, G. (2013), "Security for diversity: studying the effects of verbal and imagery processes on user authentication mechanisms", *Human-Computer Interaction–INTERACT 2013*, Springer Berlin Heidelberg, pp. 442-459.

Carstens, D.S., McCauley-Bell, P.R., Malone, L.C. and DeMara, R.F. (2004), "Evaluation of the human impact of password authentication practices on information security", *Informing Science: International Journal of an Emerging Transdiscipline*, Vol. 7, pp. 67-85.

McCullagh, D. (2000), "Kevin Mitnick testifies before congress", Politech, available at: www.politechbot.com/p-00969.html (accessed 25 April 2016).

## Corresponding author

Jeremiah D. Still can be contacted at: jstill@odu.edu