The password practices applied by South African online consumers: Perception versus reality

Authors:
Rika Butler[1]
Martin Butler[2]

Affiliations:
[1]School of Accountancy, Stellenbosch University, South Africa

[2]Business School, Stellenbosch University, South Africa

Correspondence to:
Rika Butler

Email:
rbutler@sun.ac.za

Postal address:
PO Box 3369, Matieland 7602, South Africa

Dates:
Received: 09 Sept. 2014
Accepted: 14 May 2015
Published: 10 July 2015

How to cite this article:
Butler, R. & Butler, M., 2015, 'The password practices applied by South African online consumers: Perception versus reality', *South African Journal of Information Management* 17(1), Art. #638, 11 pages. http://dx.doi.org/10.4102/sajim.v17i1.638

Background: The ability to identify and authenticate users is regarded as the foundation of computer security. Although new authentication technologies are evolving, passwords are the most common method used to control access in most computer systems. Research suggests that a large portion of computer security password breaches are the result of poor user security behaviour. The password creation and management practices that online consumers apply have a direct effect on the level of computer security and are often targeted in attacks.

Objectives: The objective of this study was to investigate South African online consumers' computer password security practices and to determine whether consumers' perceptions regarding their password security ability is reflected in the password creation and management practices that they apply.

Method: A Web-based survey was designed to (1) determine online consumers' perceptions of their skills and competence in respect of computer password security and (2) determine the practices that South African online consumers apply when creating and managing passwords. The measures applied were then compared to (1) the users' perceptions about their computer password security abilities and (2) the results of international studies to determine agreement and inconsistencies.

Results: South African online consumers regard themselves as proficient password users. However, various instances of unsafe passwords practices were identified. The results of this South African study correspond with the results of various international studies confirming that challenges to ensure safe online transacting are in line with international challenges.

Conclusion: There is a disparity between South African online consumers' perceived ability regarding computer password security and the password creation and management practices that they apply.

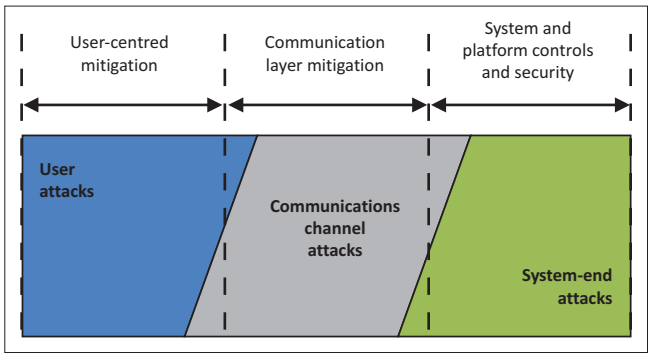
Computer password systems and vulnerability

The use of computer systems on a daily basis has changed the way in which people conduct their lives as well as their business (Shaikh & Karjaluoto 2015:541). Computer systems are accessed from users' homes, their places of employment, as well as from anywhere that they are able to access the Internet. These systems are used for business purposes, to communicate and transact over the Internet as well as for a variety of entertainment-related activities.

Stallings (1995:213) describes the use of a password system as 'the front line of defence against intruders' within a computer security environment. Having to identify oneself uniquely by way of a password before being allowed to perform certain actions has become acceptable, understandable and even expected in order to ensure a secure environment (Weber *et al.* 2008:45).

In order to control access, whilst maintaining confidentiality and integrity, user identification and authentication are essential to ensure computer security (Conklin, Dietrich & Walz 2004:1). Although other user authentication systems, such as biometrics (using physical characteristics) and one-time PINs (using device ownership), are evolving, passwords as part of security and authentication systems remain one of the most cost effective and efficient methods to use (Campbell, Kleeman & Ma 2007:2; Tam, Glassman & Vandenwauver 2010:233).

Whilst the authentication of users is critical to control access, the authentication process remains problematic (Chiasson & Biddle 2007:1). Central to the challenges concerning user authentication are the different avenues of attack used to gain unauthorised access to computer systems. The various forms of attacks to which passwords are susceptible (Figure 1) can be classified into the following (Butler 2007:520; Campbell *et al.* 2007:3; Conklin *et al.* 2004:4;



Source: Authors' own construct

FIGURE 1: Attacks to discover passwords can be aimed at various levels.

Florencio & Herley 2007:657; Notoatmodjo & Thomborson 2009:71; Tetri & Vuorinen 2013:1014):

- **System-end.** Technical or brute force attacks are launched to crack or guess the passwords of authorised users or exploit backdoors or known vulnerabilities in systems or the platforms that they use.
- **Communication channel**. Attacks on the communication channel over which passwords are transmitted by increasingly sophisticated technologies deployed at different layers of the network infrastructure.
- **User**. Attacks aimed directly at users to discover their passwords. Phishing and social engineering are increasingly popular methods of deceiving computer users into disclosing passwords.

To counter these attacks appropriate mitigation at the relevant level is necessary. Mitigation of system-end attacks should take place at the service provider level, as should mitigation of attacks on the communication channel (Butler & Butler 2014:151). However, collaboration with users of computer systems is also necessary to ensure secure transacting over networks (Figure 1). Taking cognisance of the work of Zviran and Haga (1999:164), who state that 'practically every penetration of a computer system at some stage relies on the attacker's ability to compromise a password', this research is aimed at the user level and the procedures applied (or not applied) by the computer user. According to Leach (2003:686), a large portion of the threats to passwords is the result of poor user security behaviour. When users do not select and manage passwords with care it may make those passwords easier to guess, discover or hack (Garrison 2008:70).

The responsibility of the computer user

Proper password practices refer to the execution of the policies and procedures that are used to ensure the security of passwords. Password practices encompass the measures applied when (Kothari *et al.* 2015):

- Choosing or creating passwords, which involves aspects such as the origin and composition of the password.
- Managing passwords once created (i.e. the practices relating to the safekeeping of passwords during the period of its use).

Garrison (2008:70) remarks that the 'burden' to choose a strong password (password creation) that is kept secure and confidential (password management), falls on the computer user. According to Tam *et al.* (2010:233) even the most sophisticated security system becomes useless if computer users do not apply proper password practices. Users applying proper practices when (1) creating and (2) managing passwords have a direct effect on the security of a particular computer system and the information contained in it. Although the practices of creating and managing passwords are clearly interdependent, they are viewed as distinct, yet sharing certain actions, for the purposes of this study.

Whilst certain password users may be proficient in the password creation and management practices that they apply, proper security measures and guidelines are often 'unknown, neglected, or avoided' by others (Notoatmodjo & Thomborson 2009:71). One of the reasons why many computer users apply unsafe password practices is because 'they may not know any better' due to a lack of appropriate knowledge, guidance and support (Furnell 2007:445). Researchers (Butler 2007:520; Conklin *et al.* 2004:5; Garrison 2008:70) support the argument that computer users are often ignorant and uninformed about secure password practices. Adams and Sasse (1999:42) found that ignorant users tend to 'make up their own rules' concerning passwords, which leads to the creation of 'weak' passwords or inadequate management of passwords (irrespective of whether they are 'weak' or 'strong').

However, whilst a lack of the necessary knowledge may be the reason why some computer users apply unsafe password practices, studies by Riley (2006), Tam *et al.* (2010) and Wessels and Steenkamp (2007) discovered that even users with the ability to distinguish between secure and insecure practices often don't apply these secure practices. This lack of application could stem from a lack of awareness of their vulnerability and the possible consequences related to their poor password behaviour (Gaw & Felten 2006:45).

Proper password selection entails selecting passwords that are difficult to guess but still memorable (Conklin *et al.* 2004:5; Stallings 1995:218). However, users rarely choose passwords that are both hard to guess and easy-to-remember (Yan *et al.* 2004:25). When users choose 'stronger' passwords, they are more difficult to remember and, conversely, easy-to-remember passwords are 'weaker'. This was confirmed by Zviran and Haga (1999:179), who commented on the correlation between users' difficulty with remembering passwords and password characteristics such as length, composition and lifetime – all factors that contribute to 'stronger' passwords. The conflict between convenience of remembering and security plays an important role in the quality of the passwords practices applied by computer users (Brown *et al.* 2004:650; Tam *et al.* 2010:242; Weber *et al.* 2008:46).

Florencio and Herley (2007:657) found that the average computer user has 25 password-protected accounts. As the use of password-protected systems increases, the usability of the passwords decease as human memory limitations place a strain on the memory of computer users who have to remember their numerous passwords to access these systems (Chiasson & Biddle 2007:1; Egelman *et al.* 2013). With more systems and services requiring users to identify and authenticate themselves online, the desire to select memorable passwords only increases as the number of passwords required increases. Even more disconcerting is the enforced lifetime policies and composition characteristics that in isolation (user and system) leads to stronger passwords, but at user level often leads to multiple uses of the same password (Egelman *et al.* 2013), thereby increasing risk.

Notoatmodjo and Thomborson (2009:71) refer to computer users suffering from 'password overload' and suggest that this is a major contributor to unsafe password practices. To deal with the memory challenge, users begin to devise their own methods (Adams & Sasse 1999:42), which often results in insecure password creation and management practices. Examples of such methods include: using short and weak passwords that are easy-to-remember, sharing passwords, writing down passwords and reusing passwords (Campbell *et al.* 2007:3).

Proper password practices

Since attacks on passwords can be aimed at cracking 'weak' passwords (resulting from poor password creation practices) as well as discovering or gaining access to all ('strong' and 'weak') passwords (the result of poor password management practice), it is imperative that proper password practices encompass both *creation* and *management*.

The most important criteria when *creating passwords* include the origin of the password, the characters used in its composition and the purpose of the password. Proper password creation practices include:

- **Using non-personal information:** Passwords should not use meaningful personal information such as the user's name, surname, nickname, date of birth, ID number, telephone number or any other aspect that may be associated with the user (Furnell *et al.* 2000:530).
- **Using uncommon information:** Passwords should not use words that can be found in dictionaries, acronyms or common permutations (Gehringer 2002:370).
- **Using a combination of characters:** Use a combination of uppercase and lowercase letters as well as numbers when creating passwords (Brown *et al.* 2004:650).
- **Ensuring sufficient length:** Passwords should be at least eight characters long (Garrison 2008:70).
- **Ensuring uniqueness:** Use unique passwords that are not used for other purposes (Gaw & Felten 2006:44).
- **Correlating complexity with risk:** Vary the complexity of the password to match the risk associated with its use (Brown *et al.* 2004:650).

Once users have selected a password, the *management of that password* should adhere to the following principles:

- **Single ownership:** Passwords should be kept secret and not be disclosed to or shared with other persons (Adams & Sasse 1999:41).
- **Regular changes:** Passwords should be changed regularly. The shorter the lifetime of a password, the better (Adams & Sasse 1999:41). However, although frequently changing passwords reduces the risk of undetected compromised passwords and reduces their predictability, it also hinders memorability (Zviran & Haga 1999:172).
- **Safekeeping:** Ensure proper safekeeping of passwords, including ensuring that passwords are not written down or stored in places where they could easily be discovered (Campbell, Ma & Kleeman 2011:379).
- **Single use:** Do not reuse previous passwords. When compromised in one (less secure) system, such passwords can be used to simultaneously access other systems (Gaw & Felten 2006:44).

A lack of knowledge of these password practices often leads to unsafe practices (Adams & Sasse 1999:42). However, computer users typically have different views about their skills and competence with regard to the password creation and management practices that they apply, which could contribute to users unknowingly applying improper practices (Chiasson & Biddle 2007:2).

Users' perceptions of password practices

Humans base their perceptions of performance (good or bad) on their preconceived general view about their own skills and abilities (Dunning *et al.* 2003:83; Ehrlinger & Dunning 2003:6). A phenomenon known as optimistic bias (or unrealistic optimism) often leads to an overestimation of one's own skills and competence (Weinstein 1980:806).

Covello (1983) extended the work of Weinstein for technological risk in particular and commented on the problem of overconfidence that 'leads people to believe that they are comparatively immune to common hazards'. In a similar vein, password users often overestimate their ability to create 'strong' passwords that are managed properly, whilst underestimating the potential risk associated with compromised passwords. This misconception about potential vulnerability results in poor password practices as many users believe that attackers will not be able to guess or discover their passwords (Chiasson & Biddle 2007:2).

Research objective

The objective of this study is to determine:

1. The extent to which proper password practices are applied by South African online consumers.
2. Any significant differences between the practices of South African online consumers when compared with international studies.

3. Whether consumers' perceived ability about their password practices correlates with the password practices that consumers apply.

Methodology

An online survey was designed to determine the password practices and perceived abilities from respondents for analysis. The survey instrument was refined via two iterations of pilot testing. The survey contained 43 questions which included both structured and open-ended questions. In order to ensure that users did not feel uncomfortable sharing potentially sensitive information, respondents were informed that they did not have to disclose any passwords, merely the practices that they use when creating and managing passwords. The survey was distributed to a database of online users from the authors' tertiary institution and snowball sampling was also applied. In spite of the assurances provided some respondents who were hesitant contacted the return address to confirm the validity of the study.

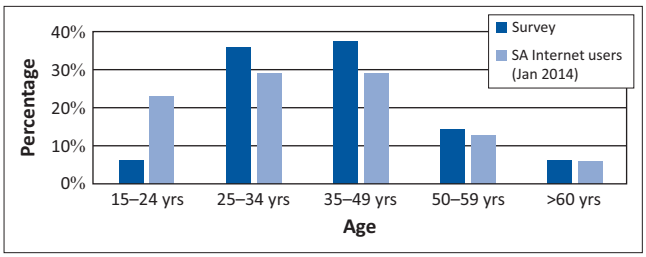
A total of 916 respondents began the survey. However, 101 respondents did not complete the survey. Excluding respondents not making use of social media or Internet banking, entrance barriers for the survey, the data set consisted of 737 responses for analysis.

The first data analysed were demographical information to determine a potential element of bias within the sample. Secondly, the practices that users apply when they select and manage passwords were analysed. These results, not detailed data, were then compared with one previous South African and multiple international studies.

To compare respondents' perceived versus actual ability a *perceived ability* score and *measured ability* score were calculated for each respondent. The perceived ability score was calculated based on respondents' self-reported ability, including their password-related knowledge. A measured ability score was calculated based on the password practices that respondents apply, as well as their ability to distinguish between different sets of passwords, varying in strength. Respondents were initially presented with a choice between two passwords from which the stronger password needed to be selected; this task increased in complexity to requiring respondents to arrange five different passwords in order of strength. After comparing the respondents' perceived ability with their measured ability, the respondents were classified as either unaware, overconfident, modest or proficient password users.

Demographics

The element of bias due to using snowball sampling was a concern. In order to express an opinion on the validity of the sample, the distribution of the gender, age and education of the respondents was compared to those of the South African Internet population. The gender distribution for



Source: IABSA, 2014b, *South African ecommerce report, effective measure/IAS South Africa Report – January 2014*, viewed 16 May 2014, from http://www.effectivemeasure.com/documents/South_Africa_Ecommerce_Report-Jan14.pdf

FIGURE 2: The age distribution of the respondents is in keeping with the South African online community.

South African online consumers is 51% female and 49% male (IABSA 2014a). This shows sufficient correlation with the survey distribution of 54% female and 46% male.

The age distribution of the sample and the South African online community (IABSA 2014b) was also compared (Figure 2). For the interval 15–24 years there is a significantly larger online population than that included in the survey. However, a significant portion of abandonment of the survey was within this younger demographic and consequently did not meet the criteria for inclusion. The age groups 25–34 and 35–49 years are both slightly over-represented, which is probably to be expected as a database of working graduates associated with the researchers' tertiary institution was used. The trend is nonetheless in line with national demographics.

The overall level of education of the respondents was quite high, with 196 respondents (21%) indicating their highest level of education as a bachelor's degree, 231 respondents (25%) an honours or postgraduate diploma, 157 (17%) a masters' degree and 30 a doctoral degree. When compared with the national demographics the postgraduate qualifications are slightly over-represented. This probably stems from the database of graduates to whom the survey was originally distributed. Even so the trend is in line with national demographics.

Based on the demographic comparison it is evident that the sample population is a reasonable, but far from perfect, fit to the South African online consumers. The slightly younger respondents are noted as well as higher than normal education levels. Although the interest in individual perceptions contrasted with reality is not influenced by any element of bias in the sample, no statistical correlation with international studies has been done. Although the researchers will present the findings as applicable to the South African online population, care must obviously be taken when extrapolating from this sample, due to an element of bias as indicated.

Online activities

Users were asked to provide an indication of their Internet experience as well as the extent of usage. Most of the respondents were experienced Internet users with 67% of

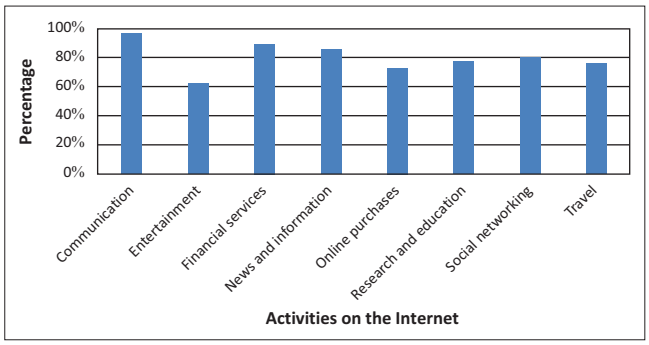


FIGURE 3: Respondents are active Internet users.

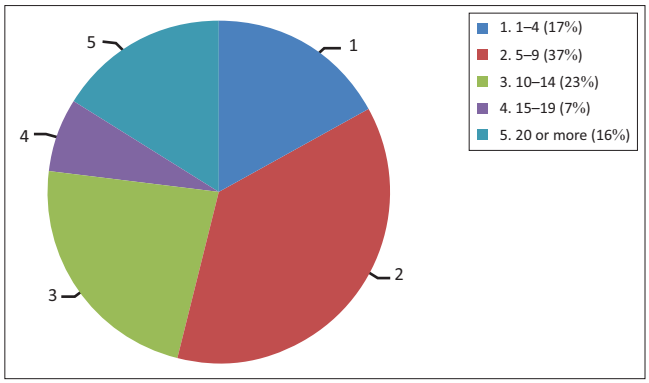


FIGURE 4: Number of Internet sites accessed that require passwords.

the respondents indicating that they have been using the Internet from the year 2000 or earlier. In response to their methods of access, most used laptop computers (84%) and mobile phones (82%). Their place of access was indicated as their residential home (90%), place of employment (83%) and always connected to the Internet via mobile access (50%). The extent of online activities indicated that 52% use the Internet equally for work and leisure, 31% mainly for work and 14% primarily for leisure.

In terms of different activities on the Internet respondents were provided with a set of choices compiled from various previous Internet surveys. The results (full sample, not only those using social media or Internet banking) show a diverse distribution of activities, with the most prevalent being communication (email, Skype, instant messaging) (96%), followed by financial services (89%) (Figure 3).

It is evident that all the respondents have been subjected to the creation and management of passwords when interacting on the Internet, as deduced from respondents when asked about the number of sites visited that require password authentication (Figure 4). A total of 83% of the respondents visit at least five sites requiring password authentication and 46% visit 10 or more sites.

The 16% of respondents who indicated 20 or more sites requiring authentication should have 20 or more passwords in the ideal situation where no passwords are reused. However, the more passwords users have, the greater the probability that they will not be used properly (Furnell 2005:10), as remembering the numerous passwords

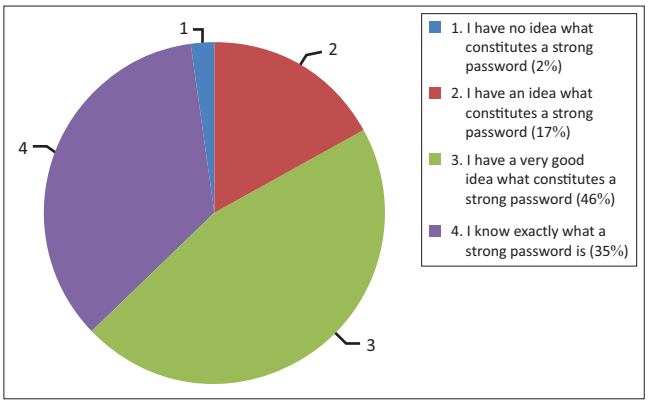


FIGURE 5: Respondents perceive that they possess the required knowledge to create strong passwords.

can prove problematic. Studies (Gaw & Felten 2006:54; Notoatmodjo & Thomborson 2009:76) have shown that the reuse of passwords increases with the number of accounts or sites that require authentication.

Findings and discussion of results

Perceived ability concerning passwords

Respondents indicate that they perceive themselves to have the required skills and competence to create strong passwords and manage them properly. Respondents were rather confident about their ability to create strong passwords (Figure 5) with 'knew exactly' (35%) and 'very good idea' (46%) how to create strong passwords being selected by more than 80% of respondents. Only 3% of the respondents had 'no idea' what constitutes a strong password.

The trend of perceived ability amongst respondents was further evident with 78% of the respondents indicating that they are comfortable about their password creation practices and 76% who felt comfortable about the password management practices that they apply. Users' potential overconfidence in ability is further supported by a question prompting respondents about their relative online 'abilities' (whilst purposefully not defining ability) where a total of 63% rated their abilities as above average, 35.5% as average and only 1.5% below average.

Measured passwords creation and management practices

Despite users' perception that they were proficient in their ability to apply proper password practices, this study found that many respondents apply unsafe password creation and management practices.

Selecting passwords

The majority of the respondents considered both convenience and security when creating new passwords. However, 'ease of remembering' was regarded by more respondents as the most important consideration when compared with 'strength' of passwords being the foremost consideration.

Convenience-orientated practices that are used when creating new passwords include using personally meaningful words (61%), personally meaningful numbers or dates (45%) and personally meaningful combinations of letters (31%). Less popular, but still present, practices were letters sequential in the alphabet (3%), sequential numbers (10%), letters consecutive on keyboards (3%), numbers consecutive on keyboards (4%) and special characters or symbols consecutive on keyboards (4%).

These results correlate with international studies which found that users often compromise security by choosing passwords that contain information that is personally meaningful to the user in order to enhance their memorability (Zviran & Haga 1999:165). Tam *et al.* (2010:242) found that 36% of their respondents were willing to sacrifice security for the ease of remembering a password. Campbell *et al.* (2007:4) determined that even the enforcement of password composition guidelines and restrictions does not discourage users from using meaningful information to create passwords.

Brown *et al.* (2004:646) determined that 83% of passwords that the respondents to their study used were derived from information about themselves or those close to them (such as nicknames, relatives, friend, pet, meaningful dates and numbers). A study by Riley (2006) indicated that more than 50% of the respondents use personally meaningful words (such as names of children and pets) when creating passwords, whilst 55% indicated that they use personally meaningful numbers (such as telephone numbers and birth dates). Studies by both Campbell *et al.* (2007:7) and Wessels and Steenkamp (2007:13) indicated that 54% of the respondents choose passwords containing meaningful information or consisting of a combination of meaningful information.

Although all the respondents use lowercase letters, the usage of different character sets decreases with numbers (98%), uppercase (85%) and special characters (67%) in use. Brown *et al.* (2004:646) found that 36% of passwords contained only alphabetical characters, 36% were numeric and 25% of their respondents' passwords consisted of alphanumeric characters. Research by Zviran and Haga (1999:170) found that users tend to avoid non-alphanumeric characters in their passwords with more than 80% of the respondents preferring to use only alphabetical characters in their passwords. This is not the case for the sample population where only 33% do not use special characters.

In a study by Riley (2006), 8% used uppercase letters, 86% of the respondents used lowercase letters, whilst 57% reported that they use numbers or digits in the passwords that they create. In all instances the usage of combinations of character sets seems to indicate a higher degree of complexity than what was indicated by previous international research. This could be an indication of more modern controls (since Zviran and Haga's 1999 research) enforcing the use of these characters.

Risk awareness and impact on passwords

Although researchers advise that the complexity of a password be varied to match the purpose of the password, the study indicates that the 'perceived risk associated with a site' is not that important a consideration for users when creating new passwords. It was indicated as the most important consideration by 18% of the respondents and the second most important by 16%. When compared to 44% of the respondents who indicated that 'ease of remembering' the password was the most important consideration and 23% who indicated this as the second most important consideration, it is clear that, although it is considered, the purpose of the password is less important to users than choosing a password that is convenient to remember.

Riley (2006) found that nearly 60% of respondents do not vary the complexity of their passwords depending on the nature of the purpose of the password. This is contradicted by Florencio and Herley (2007:660), who state that users use passwords of varying strength, depending on the importance of the information related to the accounts that they aim to protect. Their research indicates that users tend to reuse weaker passwords at more websites as opposed to the reuse of stronger passwords. This practice is fairly common in users who are risk-conscious as they tend to use one stronger password for a single or limited number of high-risk authentications (e.g. Internet banking), but another less secure password or passwords for a combination of other sites and purposes.

Password sharing and safekeeping

One of the foundations of a password system is that passwords are kept secure. However, 52.1% of the respondents to the survey indicated that they have shared a password with another person. This password sharing culture is further strengthened by the fact that 51.7% of the respondents also indicated that they know the password to an account or system that is not their own. The results of the South African study correlates with a study by Teer, Kruck and Kruck (2007:109), who found that 53% of users intentionally share their password with another person. In their study, Tam *et al.* (2010:235) found that 42% of their respondents were willing to share their passwords with trusted persons, such as friends or family members.

Forgotten passwords and password mix-ups are common (Florencio & Herley 2007:663). Although 68% of the respondents to the survey indicated that they rely on their memory to remember their passwords, 82% of the respondents indicated that they have experienced trouble remembering a password. This is more than the results of a study by Brown *et al.* (2004:647), which found that 31% of respondents have forgotten and 23% have mixed up their passwords.

Gaw and Felten (2006:50) examined the methods used to store passwords and found that whilst the majority of the

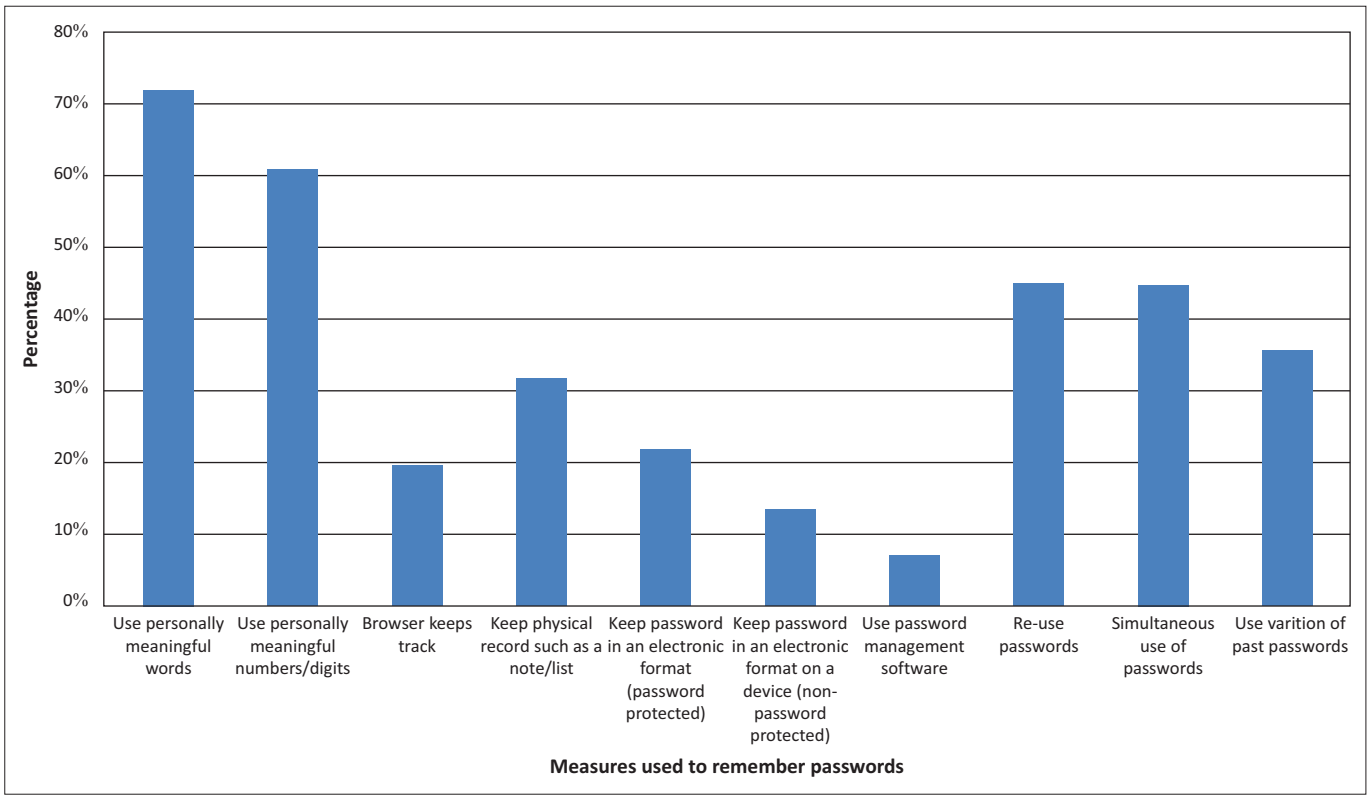


FIGURE 6: Respondents employ various practices to remember passwords.

respondents rely on their memory, respondents also applied other measures to remember and store their passwords. Figure 6 indicates the various practices that respondents use to help them remember their passwords.

Using meaningful words was indicated as the most popular technique (73%), followed by using meaningful numbers (62%). A rather significant number of respondents (19%) have designed their own measure, a protected electronic list of their passwords. This contrasts sharply with the least used method, namely password management software (6%), which provides the same, but a commercial and probably more secure concept. Two of the least secure measures, using a browser to help them keep track of their passwords (18%) and keeping a non-password-protected record (14%), are used by some users. However, when compared to previous studies, which indicated 55% (Brown *et al.* 2004:648) and 50% (Adams & Sasse 1999:42) who kept written records of their passwords, this figure is below the international trend.

Changing and reusing passwords

The requirement to change passwords regularly was tested for Internet banking, which is the highest risk activity performed by 93% of respondents. Although respondents are aware of the need to change passwords (45%), only 23% do actually regularly change their passwords. Of the respondents, 93 (13%) indicated that they have personally suffered a security breach in the past. Alarmingly, 13% of those who personally suffered breaches did not change their passwords. Password behaviour for Internet banking

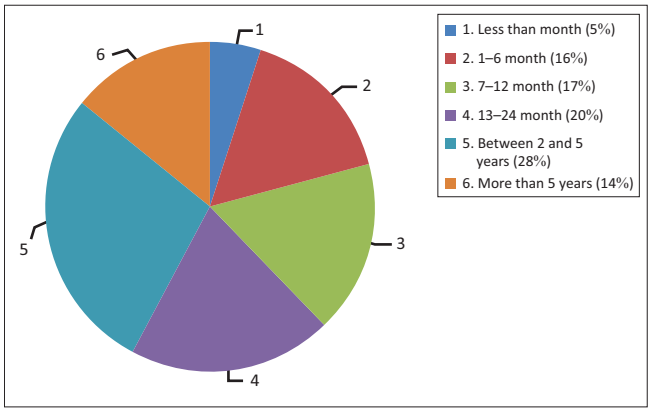


FIGURE 7: Internet banking passwords are not changed regularly.

users shows 64% of respondents have not changed their passwords in the last year and 42% not within the last two years (Figure 7).

Nearly 53% of the respondents to the Riley (2006) survey indicated that they do not change their passwords unless the system forces them to do so and Zviran and Haga (1999:172) found that nearly 80% of their respondents never changed their passwords. These findings are supported by Wessels and Steenkamp (2007:11), who found that 68% of the respondents never change their passwords if not forced to do so. Riley found that the average length of time users have maintained their primary personal use password was approximately two years and seven months.

An interesting dynamic emerges from the data and previous research. When users are not forced to change their passwords,

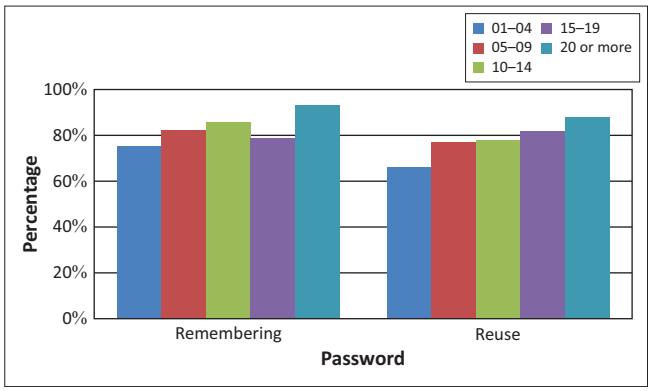


FIGURE 8: Problems remembering passwords and password reuse increase with the number of Internet sites accessed.

it rarely happens and creates a situation where passwords could potentially be reused, leading to less secure practices. However, forcing regular password changes lead to password overload and also contributes to poor password management practices. Another factor impacting practices is the total number of passwords required. Gaw and Felten (2006:54) found that the more accounts users have, the more likely they are to reuse their passwords. These researchers predict that password reuse rates will continue to rise over time, due to the pressure placed on the memories of users when they have more accounts (i.e. more passwords to remember).

Remembering passwords becomes an increasing challenge for users accessing more sites (Figure 8). Conversely, reuse of passwords also increases with the number of sites visited, confirming the conclusion of previous studies that more instances of authentication lead to weaker password creation and management practices. The data clearly indicates that users do not select unique passwords for all accounts and purposes. An alarming 75% of the respondents indicated that they reuse past passwords and 88% have simultaneously used a password for more than one purpose. Reusing passwords (43%), using the same password simultaneously (45%) and using a variation of a past password (35%) were indicated by the respondents as techniques used to help them with password overload.

Brown *et al.* (2004:647) determined that almost all the respondents reused passwords to gain access to at least one other account. In addition they found that 39% of the respondents simultaneously used one password to gain access to more than one account or system and that nearly two out of three passwords chosen by users involved duplications. According to Riley (2006), 55% of the respondents indicated that they use the exact same password for more than one account 'very frequently' or 'always' and 33% use some form of variation of the same password for multiple accounts. Gaw and Felten (2006:44) found that the majority of their respondents reused their passwords at least twice. Studies by Riley as well as Florencio and Herley (2007) found that an increasing number of users have a set of predetermined passwords that they frequently use.

A study by Taiabul Haque, Wright and Scielzo (2014:873) found that users classify passwords into different levels according to the perceived importance of the site and vary their password practices based on this classification. The results of this study supports these research findings and indicate that South African users are more cautious regarding their Internet banking password. Whilst respondents are currently using their Internet banking passwords (20%) for access to other sites, 12% have reused their Internet banking password in the past, but have stopped this practice and 69% of users have never used their Internet banking password to access other sites.

Notoatmodjo and Thomborson (2009:76) found that 37% of their participants reused passwords for high importance accounts compared to 68% who reused passwords for less important accounts. This correlation between reuse and the importance of the password purpose was also evident from this South African study (Figure 8), indicating an element of risk awareness and different practices associated with different levels of perceived risk. However, the survey indicated a potential higher level of care when dealing with Internet banking passwords (69% have never used it for another purpose) compared to the international norm.

Summary of poor practices compared with international research

Most of the results and trends regarding poor password practices that were evident from this survey show consistency with international studies (Table 1). A major

TABLE 1: Comparison of summary of poor password practices evident from this study with international studies.

Poor password practice	Result of study for South African online consumers	Comparative international studies
Convenience and security trade-off	Convenience is more important than security of passwords for many users.	Tam *et al.* (2010:242); Zviran and Haga (1999:165).
Use personally meaningful information	Use of personally meaningful words, numbers, dates, as well as sequential letters and numbers, is prevalent.	Campbell *et al.* (2007:7); Riley (2006); Brown *et al.* (2004:646).
Composition of passwords	Despite the fact that only uppercase or lowercase or alphabetical or numerical letters are used (and not combinations), the South African trend seems better that the international norm.	Zviran and Haga (1999:170); Brown *et al.* (2004:646); Riley (2006).
Insufficient consideration of perceived risk	Only 18% considers perceived risk as the most important and 16% as the second most important aspect when creating new passwords.	Riley (2006); Notoatmodjo and Thomborson (2009:76).
Password sharing	A common practice reported by the majority of the respondents.	Teer *et al.* (2007:109); Tam *et al.* (2010:235).
Changing passwords regularly	Most respondents only change passwords when forced and previous passwords are still used for high-risk environments.	Riley (2006); Zviran and Haga (1999:172).
Reuse of passwords	88% have simultaneously used a password for more than one purpose and 20% are currently using their Internet banking password to access other sites.	Florencio and Herley (2007); Brown *et al.* (2004:647–648); Gaw and Felten (2006:44, 54).

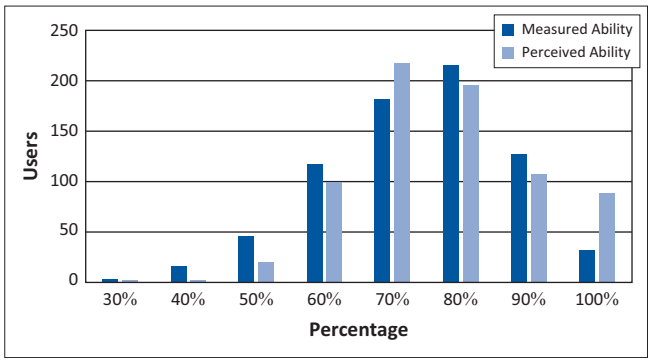


FIGURE 9: Comparison of respondents' perceived ability and measured ability.

difference observed between data in this study and previous international studies, was the extensive use of different combinations of character sets by South African consumers.

With results in line with international trends the focus moves to the final research objective, namely establishing whether users have an accurate self-awareness of their own ability (or inability) in respect of computer password security. Any change in behaviour commences with self-awareness. Hence, improving users' behaviour will require an accurate view of their existing knowledge regarding password-related matters.

Perceived ability versus measured ability

Although the majority of South African online consumers feel that they are proficient Internet users who are able to apply proper password practices, the results from the survey clearly indicate that users tend to apply unsafe password creation and management practices and are consequently not as skilled as they may perceive themselves to be.

Comparing measured ability scores and perceived ability scores

An interesting trend emerges from the comparison between users' measured ability and their perceived ability (Figure 9). For the first four intervals (<30%–60%), it seems that users underestimate their ability. Then an interesting reverse in the trend is evident in the last four intervals (70%–100%), where users mostly overestimate their perceived ability when compared to their measured ability. This poses an interesting question of whether looking at individual users' perceived ability and measured ability, rather than summarising this observed variance for the group as a whole, would provide a different view.

Classification of online consumers based on their password behaviour

Using a proficiency level of 70% for both perceived and measured ability, the responses of individual users were analysed and their ability was classified as either sufficient or insufficient. A matrix was used to plot users' perceived

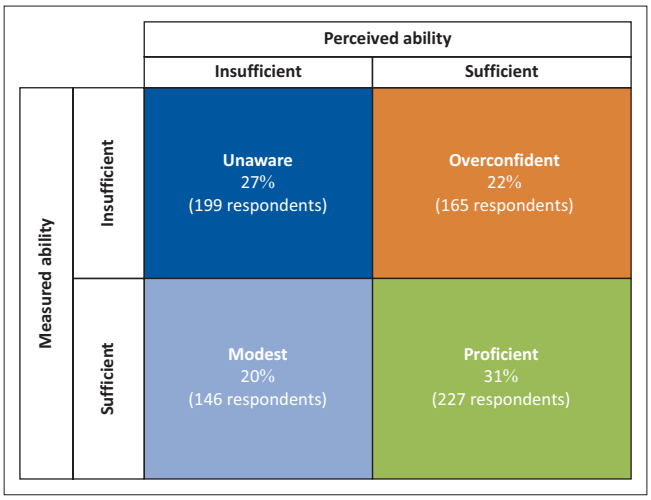


FIGURE 10: Classification of respondents as unaware, overconfident, modest or proficient after comparing their measured ability with their perceived ability.

online security abilities (sufficient or insufficient) compared to their measured ability (sufficient or insufficient). Based on this analysis respondents were divided into four different categories (Figure 10):

- **Unaware** – although they correctly perceive themselves as not being sufficiently capable, in this case ignorance is not necessarily bliss. The practices applied by these users could lead to compromised systems and resultant losses.
- **Overconfident** – users reported adequate ability, yet measured ability is not sufficient. By being overly optimistic about their abilities they are probably not that keen on improving their knowledge and as such could be the most vulnerable group.
- **Modest** – users that do not rate their own ability as sufficient, yet the measured ability indicates proficiency. On the plus side these users' lack of ability may lead to a very conservative approach, which could make them behave in a more secure manner.
- **Proficient** – the group of respondents that correctly assessed their perceived ability when compared with their measured ability. These users practice sufficiently secure password behaviour. The ideal state.

Although the sample variance when perceived and measured ability were compared (Figure 9) seems rather small, when viewed at an individual user level (Figure 10) it is clear that there is a pronounced lack of alignment between users' perceived ability and measured ability.

Conclusion

It is the 'burden' of the computer user to choose a strong password that is kept secure and confidential (Garrison 2008:70). Unfortunately, the results of this study identify and confirm some alarming facts about the extent to which users 'deal' with this burden. Disturbingly, it also raises a new concern about the lack of users' self-awareness about their computer password practices, which could hamper initiatives to improve system security.

Despite the fact that users' perceived ability indicated that they are able to create strong passwords and that strength was considered an important aspect when creating new passwords, this study found that respondents apply unsafe password creation practices. In addition, whilst respondents felt comfortable with the measures that they apply to keep their passwords safe, the use of insecure password management practices was evident.

The password practices applied by the South African respondents are fairly consistent with those observed by international studies. The main exceptions, both positive, are the clear difference in the usage of respondents' Internet banking passwords (exceeding international trends in terms of regular changes and reuse) as well as the use of a combination of different character sets, which are significantly higher than those indicated by international studies. It should be noted that the comparative studies are dated and that users' behaviour may change over time, for the better.

Optimistic bias was, however, very evident amongst South African online consumers when comparing their perceptions about their passwords creation and management practices with the password practices that they apply. For a significant number of respondents who indicated a level of comfort with their proficiency in terms of secure password behaviour, this confidence was not supported by their measured ability. This raises a rather serious concern about potential improvements in their behaviour since these users are unaware of the need to improve their password creation and management practices.

Clearly any effective measures aimed at improving the deficiencies in computer user password security identified by this research should take cognisance of the gap between users' perceptions and reality. Addressing this gap is paramount to improving computer password security. The process to address this problem should start by recognising that there are different challenges for different users (Figure 10). Uniform educational improvement programmes would therefore not be appropriate. Further research to shed light on the reasons for the lack of alignment between users' perceived and measured ability, as well as potential demographic factors that may relate to the poor alignment, is recommended.

Acknowledgements

Competing interests

The authors declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this article.

Authors' contributions

M.B. (Stellenbosch University) and R.B. (Stellenbosch University) contributed equally to the research effort in terms of design, execution, analysis and publication.

References

Adams, A. & Sasse, M.A., 1999, 'Users are not the enemy', *Communications of the ACM* 42(12), 41–46. http://dx.doi.org/10.1145/322796.322806

Brown, A.S., Bracken, E., Zoccoli, S. & Douglas, K., 2004, 'Generating and remembering passwords', *Applied Cognitive Psychology* 18(6), 641–651. http://dx.doi.org/10.1002/acp.1014

Butler, R., 2007, 'A framework of anti-phishing measures aimed at protecting the online consumer's identity', *The Electronic Library* 25(5), 517–533. http://dx.doi.org/10.1108/02640470710829514

Butler, R. & Butler, M.J., 2014, 'An assessment of the human factors affecting the password performance of South African online consumers', in *Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014)*, Plymouth, UK, July, pp. 150–161.

Campbell, J., Kleeman, D. & Ma, W., 2007, 'The good and not so good of enforcing passwords composition rules', *Information Systems Security* 16(1), 2–8.

Campbell, J., Ma, W. & Kleeman, D., 2011, 'Impact of restrictive composition policy on user password practices', *Behaviour & Information Technology* 30(3), 379–388. http://dx.doi.org/10.1080/10658980601051375

Chiasson, S. & Biddle, R., 2007, 'Issues in user authentication', *CHI Workshop Security User Studies Methodologies and Best Practices,* viewed 28 June 2014, from http://chorus.scs.carleton.ca/wp/wp-content/papercite-data/pdf/chiasson2007issues-chiworkshop.pdf

Conklin, A., Dietrich, G. & Walz, D., 2004, 'Password-based authentication: A system perspective', in *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, Hawaii, January 5–8, 2004, pp. 1–10. http://dx.doi.org/10.1109/hicss.2004.1265412

Covello, T.V., 1983, 'The perception of technological risks: A literature review', *Technological Forecasting and Social Change* 23(4), 285–297. http://dx.doi.org/10.1016/0040-1625(83)90032-X

Dunning, D., Johnson, K., Ehrlinger, J. & Kruger, J., 2003, 'Why people fail to recognize their own incompetence', *Current Directions in Psychological Science* 12, 83–87. http://dx.doi.org/10.1111/1467-8721.01235

Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K. & Herley, C., 2013, 'Does my password go up to eleven? The impact of password meters on password selection', in *Proceedings of the Conference on Human Factors in Computing Systems*, Paris, France, May, 2013, pp. 2379–2388. http://dx.doi.org/10.1145/2470654.2481329

Ehrlinger, J. & Dunning, D., 2003, 'How chronic self-views influence (and potentially mislead) estimates of performance', *Journal of Personality and Social Psychology* 84(1), 5–17. http://dx.doi.org/10.1037/0022-3514.84.1.5

Florencio, D. & Herley, C., 2007, 'A large-scale study of Web password habits', in *Proceedings of the 16th international conference on World Wide Web*, Banff, Canada, May, 2007, pp. 657–666. http://dx.doi.org/10.1145/1242572.1242661

Furnell, S.M., 2005, 'Authenticating ourselves: Will we ever escape the password?', *Network Security* 3, 8–13. http://dx.doi.org/10.1016/S1353-4858(05)00212-6

Furnell, S.M., 2007, 'An assessment of website password practices', *Computers and Security* 26, 445–451. http://dx.doi.org/10.1016/j.cose.2007.09.001

Furnell, S.M., Dowland, P.S., Illingworth, H.M. & Reynolds, P.L., 2000, 'Authentication and supervision: A survey of user attitudes', *Computers and Security* 19, 529–539. http://dx.doi.org/10.1016/S0167-4048(00)06027-2

Garrison, C.P., 2008, 'An evaluation of passwords', *CPA Journal*, 70–71.

Gaw, S. & Felten, E.W., 2006, 'Password management strategies for online accounts', in *Proceedings of the 2nd Symposium of Usable Privacy and Security*, Pittsburgh, P.A., July, pp. 44–55. http://dx.doi.org/10.1145/1143120.1143127

Gehringer, E.F., 2002, 'Choosing passwords: Security and human factors', in *Proceeding of the 2002 International Symposium on Technology and Society*, Raleigh, N.C., June, pp. 369–373. http://dx.doi.org/10.1109/istas.2002.1013839

Interactive Advertising Bureau of South African (IABSA), 2014a, *Effective measure data for January 2014*, viewed 16 May 2014, from http://www.iabsa.net/research/effective-measure-data-for-january-2014

IABSA, 2014b, *South African ecommerce report, effective measure/IAS South Africa Report – January 2014*, viewed 16 May 2014, from http://www.effectivemeasure.com/documents/South_Africa_Ecommerce_Report-Jan14.pdf

Kothari, V., Blythe, J., Smith, S.W. & Koppel, R., 2015, 'Measuring the security impacts of password policies using cognitive behavioral agent-based modelling', in *Proceedings of the 2015 Symposium and Bootcamp on the Science of Security*, Urbana, I.L., April 2015, pp. 13–22.

Leach, J., 2003, 'Improving user security behaviour', *Computers and Security* 22(8), 685–692. http://dx.doi.org/10.1016/S0167-4048(03)00007-5

Notoatmodjo, G. & Thomborson, C., 2009, 'Passwords and perceptions', in *Proceedings of the Australasian Information Security Conference (AISC2009)*, Wellington, January, 2009, Conferences in Research and Practice in Information Technology, 98, pp. 71–78.

Riley, S., 2006, 'Password security: What users know and what they actually do', *Usability News* 8(1), viewed 18 August 2012, from http://psychology.wichita.edu/surl/usabilitynews/81/Passwords.asp

Shaikh, A.A. & Karjaluoto, H., 2015, 'Making the most of information technology & systems usage: A literature review, framework and future research agenda', *Computers in Human Behavior* 49, 541–566. http://dx.doi.org/10.1016/j.chb.2015.03.059

Stallings, W., 1995, *Network and internetwork security principles and practice*, Prentice Hall, Englewood Cliffs.

Taiabul Haque, S.M., Wright, M. & Scielzo, S., 2014, 'Hierarchy of users' web passwords: Perceptions, practices and susceptibilities', *International Journal of Human-Computer Studies* 72(12), 860–874. http://dx.doi.org/10.1016/j.ijhcs.2014.07.007

Tam, L., Glassman, M. & Vandenwauver, M., 2010, 'The psychology of password management: A tradeoff between security and convenience', *Behaviour & Information Technology* 29(3), 233–244. http://dx.doi.org/10.1080/01449290903121386

Teer, F.P., Kruck, S.E. & Kruck, G.P., 2007, 'Empirical study of students' computer security practices/perceptions', *Journal of Computer Information Systems* 47(3), 105–110.

Tetri, P. & Vuorinen, J., 2013, 'Dissecting social engineering', *Behaviour and Information Technology* 32(10), 1014–1023. http://dx.doi.org/10.1080/0144929X.2013.763860

Weber, J.E., Guster, D., Safanov, P. & Schmidt, M.B., 2008, 'Weak password security: An empirical study', *Information Security Journal: A Global Perspective* 17(1), 45–54.

Weinstein, N.D., 1980, 'Unrealistic optimism about future life events', *Journal of Personality and Social Psychology* 39, 806–820. http://dx.doi.org/10.1037/0022-3514.39.5.806

Wessels, P.L. & Steenkamp, L., 2007, 'Assessment of current practices in creating and using passwords as a control mechanism for information access', *South African Journal of Information Management* 9(2), 17 pages.

Yan, J., Blackwell, A., Anderson, R. & Grant, A., 2004, 'Password memorability and security: Empirical results', *Security and Privacy* 2(5), 25–31. http://dx.doi.org/10.1109/MSP.2004.81

Zviran, M. & Haga, W.J., 1999, 'Password security: An empirical study,' *Journal of Management Information Systems* 15(4), 161–185.