South African Journal of Information Management
ISSN: (Online) 1560-683X, (Print) 2078-1865

Some password users are more equal than others: Towards customisation of online security initiatives

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

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

[2]University of Stellenbosch Business School, Stellenbosch University, South Africa

Corresponding author:
Rika Butler,
rbutler@sun.ac.za

Dates:
Received: 12 Oct. 2017
Accepted: 23 May 2018
Published: 31 July 2018

How to cite this article:
Butler, R. & Butler, M., 2018, 'Some password users are more equal than others: Towards customisation of online security initiatives', *South African Journal of Information Management* 20(1), a920. https://doi.org/10.4102/sajim.v20i1.920

Copyright:
© 2018. The Authors. Licensee: AOSIS. This work is licensed under the Creative Commons Attribution License.

Read online:
Scan this QR code with your smart phone or mobile device to read online.

Background: Online security is a growing concern and user authentication through passwords remains an important mechanism to protect online assets. Research to date has highlighted the need to address human behaviour but without an indication of where the emphasis of security education, training and awareness (SETA) initiatives should be, beyond improved password practices.

Objectives: The aim of this study was to, through analysis of the password behaviour of South African online consumers: (1) understand the prevalence of poor password practices among consumers overall and (2) identify specific password deficiencies prevalent among different demographic groups to be focus areas for tailored intervention programmes.

Method: The study uses a quantitative research approach. An online survey was used to gather demographic data, perceptions about online security and applied password practices. A sample of 737 valid responses was analysed for this research.

Results: Based on the descriptive analysis of the responses three key observations were made. Firstly, there is a distinct difference in the incidence of poor password practices for all respondents and thus support for tailored interventions. Secondly, there are variances between the practices within different demographic groups that could be used for customisation of interventions. Finally, the different poor practices cannot be uniquely attributed to one particular set of demographics.

Conclusion: The study concluded that to improve computer password security in South Africa, password SETA programmes should be customised for areas where individual needs exist and not merely per password practice or demographic group.

Introduction

The growth in the use of computers and the Internet have increased the number of threats computer users are exposed to. Although the South African Cyber Security Policy Framework (South Africa 2015) aims to foster a cyber-security culture, it does not include provision for security education, training and awareness (SETA), which are regarded as critical components to foster such a culture (Kortjan & Von Solms 2014:30).

Varying levels of digital literacy among computer users and different behaviour by users in the online environment make it difficult to apply a uniform set of interventions to improve security behaviour. Researchers (Chandarman & Van Niekerk 2017; McCormac et al. 2017) have emphasised the importance of appropriate interventions to address the weaknesses of particular target audience groups. This is supported by Kruck and Teer (2008:80), who recommend that those responsible for computer SETA gain 'a better understanding' of areas where deficiencies in computer security are present.

For decades, user identification and authentication have been regarded as the foundation of computer security (Conklin, Dietrich & Walz 2004:1), playing an important role in securing information. Despite the evolution of other methods of identification and authentication of computer users, such as biometrics, single sign-on and one-time pin, the use of passwords remains the most common way to control access and authenticate computer users (Das et al. 2014; Tam, Glassman & Vandenwauver 2010). However, passwords are increasingly subject to various forms of attack (Shen et al. 2016:131), making proper computer password security essential.

Ensuring proper computer password security involves both technological and human aspects (Brostoff & Sasse 2002:41). While technology can provide a certain level of protection against

certain threats, human behaviour remains a potential weak link. The 'burden' of choosing a strong password that is kept secure and confidential remains on the computer user (Garrison 2008:70) and even the most sophisticated systems become inadequate if computer users do not apply proper password practices (Tam et al. 2010:233).

Butler and Butler (2014:159) recommend that initiatives to educate, train and raise awareness take cognisance of the particular aspects that influence password behaviour. Studies by McCrohan, Engel and Harvey (2010) have demonstrated that specific training on relevant password-related matters improved users' password behaviour significantly. The objective of this research is to determine if there are varying levels of proficiency regarding password practices between different demographical groups that could direct the tailoring of such initiatives.

Important elements to be considered in the design of any SETA initiatives include the target audience, the relevant topics, the content and the method of communication (Kortjan & Von Solms 2014:33). To present the appropriate audience with applicable SETA content, it is necessary to examine user password practices and identify deficiencies in performance among the various groupings of users. These factors can then be emphasised in tailored SETA programmes (Kruger et al. 2008:56) to ensure that audiences targeted with these initiatives are presented with relevant content, delivered by appropriate mechanisms. The importance of relevance in education to bring about behavioural change is well documented, including in the field of information security (Soomro, Shah & Ahmed 2016:216).

Literature review

Online security

The password practices that users apply have a direct effect on the level of security of computer systems. While certain password users are proficient in their password practices, proper security measures and guidelines are often 'unknown, neglected, or avoided' by other computer users (Notoatmodjo & Thomborson 2009:71). Garrison (2008:70) determined that many computer users are ignorant and uninformed about how to select usable and secure passwords. In addition, many computer users are unaware of their vulnerability and the possible consequences associated with improper password use and control. Chandarman and Van Niekerk (2017:134) regard the untrained user as one of the weakest links in a security system.

Security should be a foremost concern when creating new passwords (Huth, Orlando & Pesante 2012; Zhang-Kennedy, Chiasson & Van Oorschot 2016). Ominously, human memory limitations place a strain on computer users' memory and they experience difficulties in remembering numerous passwords (Furnell & Esmael 2017:5; Shen et al. 2016:131). Notoatmodjo and Thomborson (2009:71) refer to this as 'password overload', a term widely used in the literature, which often results in weak password behaviour. Yan et al. (2004:25) found that many users rarely choose passwords that are both hard to guess and easy to remember. A conflict between two opposing principles, convenience (memorability and usability) and security, therefore, exists.

Poor password practices

Kothari et al. (2015:15) reasoned that password practices encompass the measures that computer users apply when choosing or creating passwords (which involves aspects such as the origin of the password and the characters used in its composition), as well as managing passwords (measures that relate to the safekeeping of passwords). Groupings of common proper and improper password practices that were the topic of various studies are presented in Table 1.

Although authors propose that interventions should focus on the educational requirements of particular target audience groups, they do not explain how to design custom-made SETA interventions. As 'very few' studies focussing on computer security awareness in South Africa have been conducted (Chandarman & Van Niekerk 2017:136), the extent to which SETA programmes should focus on the proper password practices in Table 1 remains somewhat elusive in academic literature.

Demographics and password practices

Research into computer security often focusses on 'particular user communities' and does not necessarily report on the effects of demographics, despite the fact that basic demographic information is often obtained, and commented upon, in these studies (Howe et al. 2012:210). Some studies commented on notable differences between different demographical groupings for security in general, not passwords in particular.

While McCormac et al. (2017:152) noted small differences in individuals' information security awareness and their age and gender, Pattinson et al. (2015) found that gender has no significant influence on information security behaviour but that age seems to improve secure behaviour. Sheng et al. (2010) found minor variances between males and females and different age groups regarding susceptibility to computer security threats such as phishing. Chaudhary et al. (2015) found female respondents more susceptible to poor online behaviour, in this instance phishing attacks, than male respondents. It was found that age reduces the risk perception associated with a loss of data confidentiality (Milne, Labrecque & Cromer 2009) and increases vulnerability to threats such as spyware (Fox 2006), while males seem to have a tendency to engage in more risky online behaviour (Byrne et al. 2012).

Chen, Paik and McCabe (2014:135) reported on different levels of defensive measures taken by online consumers based on education levels. Redmiles, Kross and Mazurek (2016:666) found that users with higher education levels are significantly more likely to learn from negative experiences. These groups also have access to more credible sources

TABLE 1: Studies on common password practices.

Proper password practice indicator	Supporting studies	Improper practice	Supporting studies
Security should be the foremost concern when creating passwords.	• Huth et al. (2012) • ISACA (2010) • Singleton (2012) • Zhang-Kennedy et al. (2016)	Convenience is regarded as more important than security.	• Butler and Butler (2015) • Shen et al. (2016)
Use complex passwords in terms of composition characters used and length.	• Bonneau et al. (2015) • Campbell, Kleeman and Ma (2007) • Furnell (2007) • Shay et al. (2010) • Singleton (2012) • Turan et al. (2010) • Zhang-Kennedy et al. (2016)	Passwords not sufficiently complex.	• Shen et al. (2016) • Butler and Butler (2015) • Florencio and Herley (2007) • Riley (2006) • Zviran and Haga (1999)
Use non-meaningful information.	• Furnell (2007) • Garrison (2008) • Singleton (2012) • Turan et al. (2010) • Zhang-Kennedy et al. (2016)	Use of personally meaningful information.	• Shen et al. (2016) • Brown et al. (2004) • Butler and Butler (2015) • Campbell et al. (2007) • Riley (2006) • Shay et al. (2010)
Do not share passwords.	• Furnell (2007) • ISACA (2010) • McDowell, Hernan and Rafail (2013) • SANS (2014) • Zhang-Kennedy et al. (2016)	Password sharing.	• Butler and Butler (2015) • Furnell (2005) • Shay et al. (2010) • Taiabul Haque, Wright and Scielzo (2014) • Teer, Kruck and Kruck (2007)
Password should be unique – not reused or simultaneously used for other purposes.	• Bonneau et al. (2015) • Garrison (2008) • ISACA (2010) • SANS (2014) • Zhang-Kennedy et al. (2016)	Reuse of the same password and simultaneous *use* of password for more than one purpose.	• Brown et al. (2004) • Butler and Butler (2015) • Florencio and Herley (2007) • Furnell et al. (2000) • Gaw and Felten (2006) • Riley (2006) • Shay et al. (2010) • Brown et al. (2004) • Butler and Butler (2015) • Furnell et al. (2000) • Bonneau et al. (2015)
Regularly change passwords.	• Adams and Sasse (1999) • Furnell (2007) • SANS (2014) • Zhang-Kennedy et al. (2016)	Not regularly changing passwords.	• Butler and Butler (2015) • Furnell (2005) • Furnell et al. (2000) • Inglesant and Sasse (2010) • Riley (2006) • Teer et al. (2007)
Vary password complexity with the risk associated with its use.	• Bonneau et al. (2015) • Brown et al. (2004) • ISACA (2010) • Zhang-Kennedy et al. (2016)	Lack of perceived risk associated with use.	• Butler and Butler (2015) • Riley (2006)
Store passwords securely.	• Bonneau et al. (2015) • SANS (2014) • Zhang-Kennedy et al. (2016)	Use of unsafe password storing practices.	• Adam and Sasse (1999) • Brown et al. (2004) • Butler and Butler (2015) • Gaw and Felton (2006)

Note: Please see the full reference list of the article, Butler, R, Butler, M., 2018, 'Some password users are more equal than others: Towards customisation of online security initiatives', *South African Journal of Information Management* 20(1), a920. https://doi.org/10.4102/sajim.v20i1.920, for more information.

of security-related information, potentially leading to more secure behaviour online.

The literature for demographics impacting passwords in particular is scarce. Gender as a distinguishing factor did feature in research by Bryant and Campbell (2006), determining that females are more likely to use meaningful information in the composition of their passwords, while males are more likely to use similar passwords for more than one purpose (Bryant & Campbell 2006:90). Shay et al. (2010) noted a decrease in password sharing as respondents grew older. Bryant and Campbell noted a slight decrease in respondents who did not use a proper combination of characters in the composition of passwords as age increased. The literature indicates that age does not negatively impact upon all practices; Bryant and Campbell also established that older participants were not more, or less, likely to change their passwords more often than younger users.

According to Karlsson, Åström and Karlsson (2015:246) existing research into online security has focussed on a broad set of research topics but with limited depth. More importantly, an extensive part of the research is descriptive, philosophical or theoretical, lacking a structured use of empirical data, making it quite immature.

Behavioural change

The goal of SETA interventions is to change and improve user behaviour. Although many organisations show compliance in running security awareness programmes, this does not necessarily result in a behavioural change. Merely complying, and not dealing with the actual deficiencies, can result in people being more averse to change than before, according to Skinner et al. (2018).

According to Michie and Johnston (2012), basic psychological research over the last century has demonstrated that behaviour and behavioural change follow predictable patterns and that it is, therefore, vital that interventions be guided by accumulated science. This is supported by work from Curry et al. (2018:49) indicating that the motivational antecedents of intent are separate from the volitional drivers of behaviour. They suggest that 'appropriately differentiated treatments' to support behavioural change should 'inform practical security behaviour improvement initiatives'.

User behaviour concerning passwords has a direct effect on computer security (Gehringer 2002:369). Using the determinants of human behaviour, based on the model of McCloy, Campbell and Cudeck (1994), Butler and Butler

(2014) defined three determinants for individual password performance, namely relevant knowledge of password practices, the capability to successfully combine password-related knowledge with knowing how and being able to apply proper password practices, and the motivation to behave securely. Their password performance model is used as theoretical construct for this research.

Methods

Objective of study

The primary objective of this study was to determine the individual SETA needs in South Africa by analysing the following:

- The prevalence of poor password practices, to define common SETA focus areas.
- The variance between different demographic groups to define focus areas for tailored SETA initiatives.

The results of this study are presented as relative focus areas per poor password practice (Figure 1), as well as a demographical variance heat map to indicate deficiencies in password practices displayed for different demographic groups. These results should be useful to practitioners defining appropriate SETA programmes. Future research in this space could be focussed on the complex interrelatedness of the different demographic factors that sometimes display an interesting cyclic nature, especially with years of Internet experience and number of sites visited that require authentication.

Recommendations made from the observed differences and literature on appropriate interventions make a contribution for practitioners designing SETA interventions.

Research design and measuring instrument

A survey design that targets a large sample of responses, to potentially cover different demographics across five dimensions, was deemed appropriate. Ethical clearance for the research project was obtained from the Departmental Ethical Screening Committee at the academic institution of the authors.

The following steps were followed in the research process:

- A literature study was performed to determine best practices for passwords (Table 1) and compile a list of potential deficiencies.
- A survey was designed and pilot tested to ensure accuracy and no forced answers from respondents. Because the intent was not inferential statistics and multiple questions per deficiency that would allow for statistical reliability and validity, a minimum of two rounds of pilot testing was deemed necessary to ensure question validity.
- The survey was distributed online using a commercial survey site and it was decided not to include an offline survey because the participants could be less likely to fall within the target population of password users.
- The overall password performance was analysed to determine the incidence of improper practices among the entire data set (Figure 1). For purposes of this study, the common improper practices indicated in Table 1 served as the basis to classify 'weak' password behaviour.
- Password behaviour displayed was analysed for different demographic groups (Figures 2–7).
- An analysis of the variation, for different demographics, was performed to identify areas of focus for tailored SETA programmes based on demographics (Figure 8).

Data collection and analysis

The survey instrument was pilot tested on a sample population of both technology literate and less literate users to ensure construct validity and meaning options for each question or statement. After two rounds of pilot testing and confirmation that all questions were valid, the survey was administered using an online survey tool and distributed via social media (Twitter) and institutional email. Given a desire for a large sample, yet no inferential statistics that would impose strict sampling decisions, a snowball distribution method was used.

A total of 737 useful responses were obtained for analysis. As the survey questions asked for the prevalence of the different antecedents of poor password practices as indicated in Table 1 via a single question each, statistical validity for multiple statements per construct can thus not be determined.

The analysis was conducted using descriptive statistics (Figures 2–7) and no inferential statistics to any confidence level were performed. Figure 8 represents the performance heat map, indicating the reported difference in behaviour for the different demographic groupings for three defined levels of performance.

Demographics and bias

The demographic composition of the population is presented in Table 2.

TABLE 2: Demographic composition of population.

Demographic category	Variable	Number of respondents (n = 737)	%
Age	< 35 years	307	41.6
	35–49 years	282	38.3
	50+ years	148	20.1
Gender	Male	351	47.6
	Female	386	52.4
Number of sites that require authentication	< 10	397	53.9
	10–19	224	30.4
	20+	116	15.7
Highest level of education	School level up to Grade 12	96	13.0
	Graduated with bachelor's degree or diploma	289	39.2
	Post-graduate qualification	352	47.8
Years of Internet experience	15+ years	516	70.0
	10–14 years	146	19.8
	< 10 years	51	6.9

Comparison of the demographic data with that of South African Internet users shows a potential bias in terms of education levels. This is to be expected given the method of distribution from within the database of an academic institution. Gender and age distribution was deemed representative, and no comparative data sets are available to determine potential bias in terms of the numbers of sites visited nor years of Internet experience.

Research context value contribution

Research about passwords is often conducted within a particular context, such as an organisation that the author has access to. This is often an academic institution (Kruck & Teer 2008; Yan et al. 2004) or particular industry that imposes additional regulatory challenges, like health care (Ghazvini & Shukur 2017), or where the assets protected are particularly attractive, such as financial services.

This research did not aim for, nor was it limited to, a particular context. Practitioners from a broad sphere of applications may be interested in the results. However, the intent is not to use the results to design differentiated SETA programmes but rather to acknowledge the potential difference that may exist in every context and incorporate that into a learning process design. Academics may wish to test for these differences within specific contexts.

Research results

Overall password behaviour

Analysis revealed that respondents vary significantly in their password practice proficiency levels. Furthermore, a discrepancy between users' perceptions of their password practices and the reality (practices measured) was evident. A total of 39 respondents (5.3%) perceived that they possessed absolute knowledge of proper password practices. However, only a single respondent (0.1%) was able to demonstrate flawless ability to apply proper password practices and only 21 respondents (2.8%) displayed a perfect 'security first' aptitude when selecting and managing passwords.

The password creation and management practices of respondents were analysed to distinguish between secure and weak password behaviour. Numerous instances of weak password creation and management practices were evident (Figure 1).

The most prevalent poor practices were the simultaneous use of the same passwords (90.1%) and password reuse (77.3%).

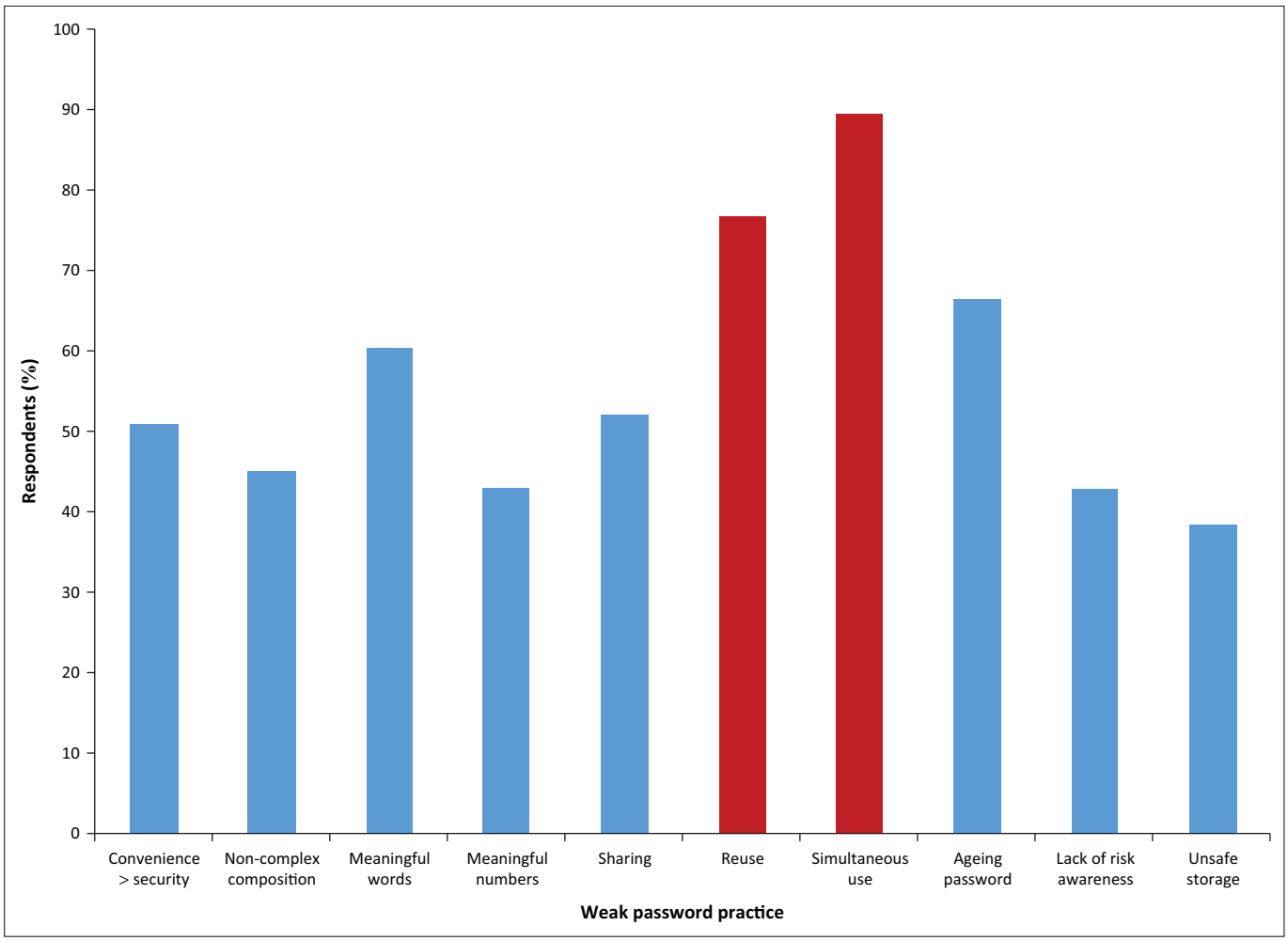

FIGURE 1: Improper password practices for total data set.

This was not unexpected because studies by Das et al. (2014) and Wash et al. (2016) highlighted that users have fewer passwords than the number of websites they visit, indicating password reuse. Shay et al. (2010) found that more than 80.0% of their respondents reused or slightly altered passwords for multiple purposes. Wash et al. concluded that 85.0% of respondents reused passwords. The reuse and simultaneous use of passwords is thus an extremely important focus area for SETA, especially where the same passwords are used to protect valuable assets (like online banking) and less valuable, and often less well-protected, Internet sites of a general nature.

Analysis of weak password behaviour per demographic group

The analysis for the customisation of SETA programmes followed a dual approach. Firstly, it was determined which of the weak password practices were more prevalent across the entire population to ensure that these aspects were highlighted across the board for all demographics (Figure 1). Secondly, the prevalence of weak password behaviour within different demographic groups was analysed. The results are presented in Figures 2–7.

Age group

Figure 2 indicates the weak password practices per age group.

The occurrence of weak behaviour decreased for the majority of practices as respondents grew older. A possible reason for this could be that older respondents do not visit as many Internet sites that require authentication with passwords as younger age groups, meaning that they do not have as many passwords to manage, resulting in less password reuse and simultaneous use. A decrease in the extent of password sharing as respondents grew older was noted, supporting the findings of Shay et al. (2010).

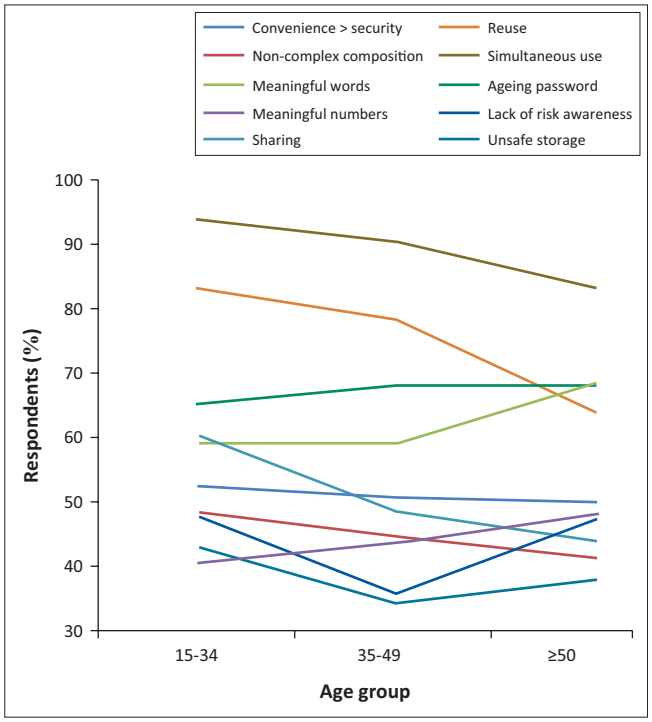

FIGURE 2: Weak password practices per age group.

A comparison between the age groups and the number of sites accessed that require authentication is shown in Figure 3. It confirms that there is indeed a decreasing trend in the percentage of older respondents who access 15 or more sites requiring authentication, which could explain the decrease in the password deficiencies identified among the older demographics. This limitation of the research does not impact the recommendations to the extent that it would, had the objective been a regression study to define the extent of each individual demographic on the performance. It merely indicates that cross-loading is evident within the selected demographics and should be investigated by future research.

While the majority of poor practices decreased with respondents' age, the practices of using personally meaningful words and numbers, not changing passwords regularly and using unsafe storing practices increased, the older the respondents were. This could indicate that although they visit fewer sites requiring authentication (Figure 3), the age group above 50 years are possibly unaware of the dangers associated with the use of personally meaningful information when creating passwords. This is supported by the increased lack of risk awareness as respondents grew older, not unexpected because older participants are not digital natives who have benefited from a lifelong digital experience, including best practice.

Gender

The results regarding the weak practices that respondents applied, analysed by gender, are contained in Figure 4. Although both genders displayed improper password practices, the areas of deficiency for male and female respondents differed.

There was no notable difference in simultaneous use and unsafe storage practices across gender. A slight variance in the prevalence of the improper practices of regarding ease more important than security when creating passwords, risk

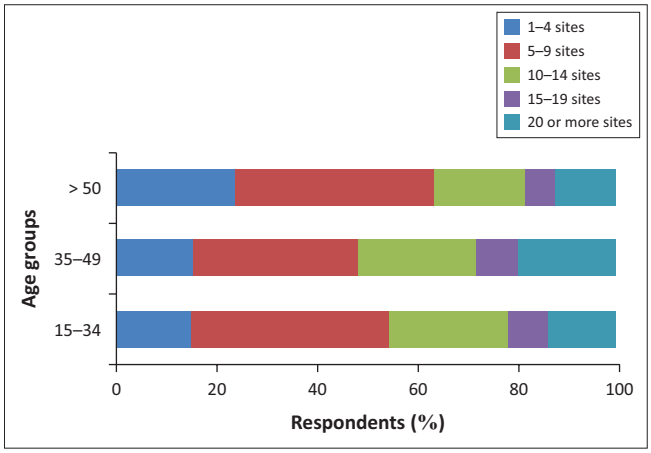

FIGURE 3: Age group versus number of sites requiring authentication.

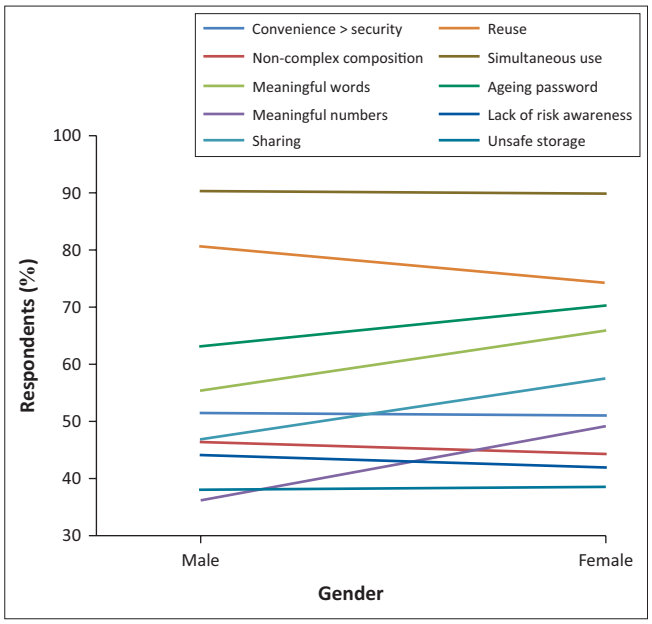

FIGURE 4: Weak password practices per gender.

not regarded as an important consideration when creating passwords, not using a proper combination of characters to create passwords and password reuse were found. Although the variance was only slight, females seem to apply these improper practices less often than males.

Although female respondents tended to reuse their passwords less than the male respondents, they were guiltier of using personally meaningful information, shared passwords more often and did not change their passwords as often as the male respondents.

When analysing the number of sites visited requiring authentication, per gender, it was found that almost a similar percentage of each gender accessed 10–14 sites and 15–19 sites. However, significantly more male respondents accessed 20 or more sites, while more females visited 1–9 different sites. Notoatmodjo and Thomborson (2009) found that the more passwords users need to acquire access to sites, the more they tend to reuse passwords. The fact that the male respondents in this study visited more sites requiring authentication could explain why they tended to reuse their passwords more, supporting the study by Bryant and Campbell (2006) but again showing some cross-loading of demographic factors on password performance for future research and analysis.

Despite Figure 4 showing that in general female respondents apply weak password practices to a greater extent than males, interestingly, more than 90% of the top 11 overall password performances indicated in this study, originated from female respondents.

Number of Internet sites accessed

Figure 5 shows the analysis of poor practices based on the number of sites that respondents visit requiring authentication using passwords.

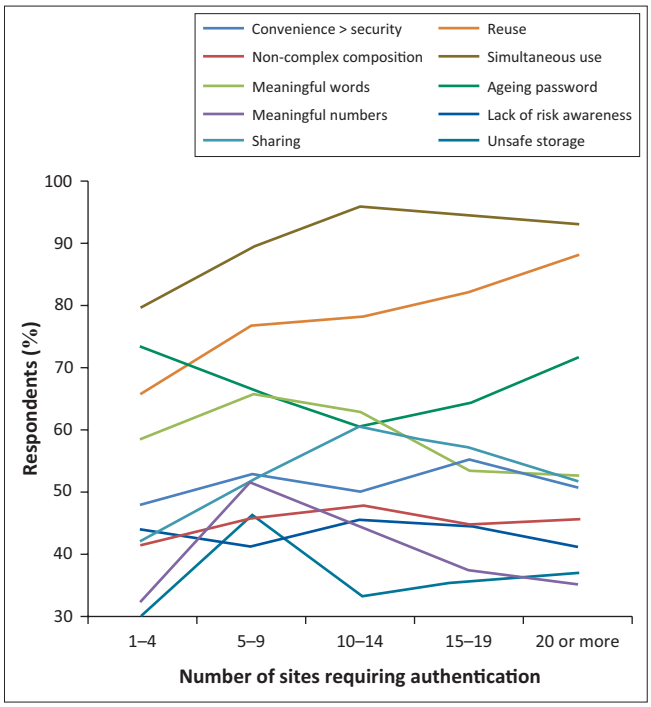

FIGURE 5: Weak password practices per number of sites requiring authentication.

This study showed that the more passwords users have, the more they tend to reuse and simultaneously use their passwords. This confirms the observations from the literature about human memory limitations (Sasse, Brostoff & Weirich 2001:124), resulting in users suffering from 'password overload' when they have more passwords to remember (Notoatmodjo & Thomborson 2009).

The results of this South African study corresponds with the results of a number of international studies that found a correlation between the number of passwords that users have and the following insecure practices that users often apply:

- password reuse (Adams & Sasse 1999:42; Carstens et al. 2004; Florencio & Herley 2007:660; Gaw & Felten 2006:48)
- the simultaneous use of a password for more than one purpose (Adams & Sasse 1999:42; Carstens et al. 2004; Florencio & Herley 2007:660; Furnell 2005:10).

The number of sites requiring authentication seems to have no significant influence on the following password creation practices: considering ease versus security, considering the risk of the password's use in its creation and the characters used in the composition of passwords. In contrast to research by Furnell (2005:10), this study did not find a distinctive increase in the use of personally meaningful information, not changing passwords regularly or password sharing as the number of passwords increases.

Education

The weak practices analysed per highest level of education appear in Figure 6. While using meaningful words was found to be the highest for graduates, using meaningful numbers increased with levels of education. Although the weak practice

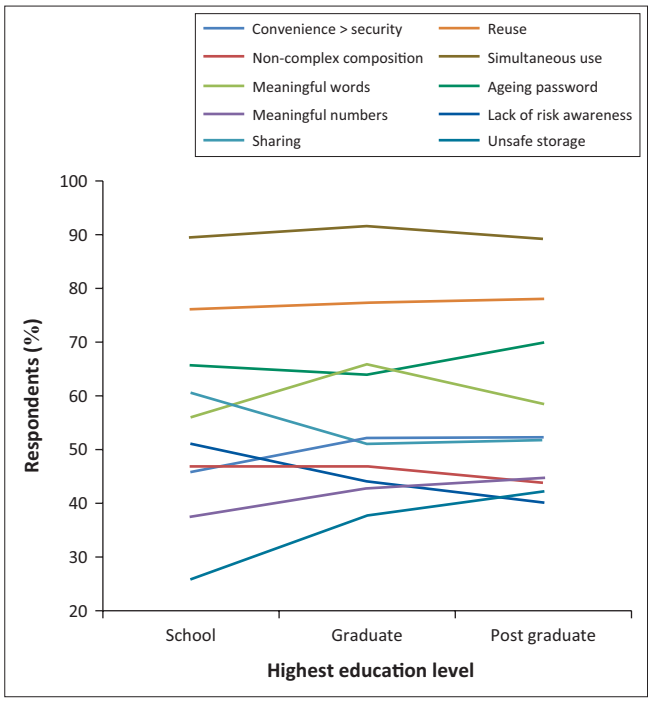

FIGURE 6: Weak password practices per highest level of education.

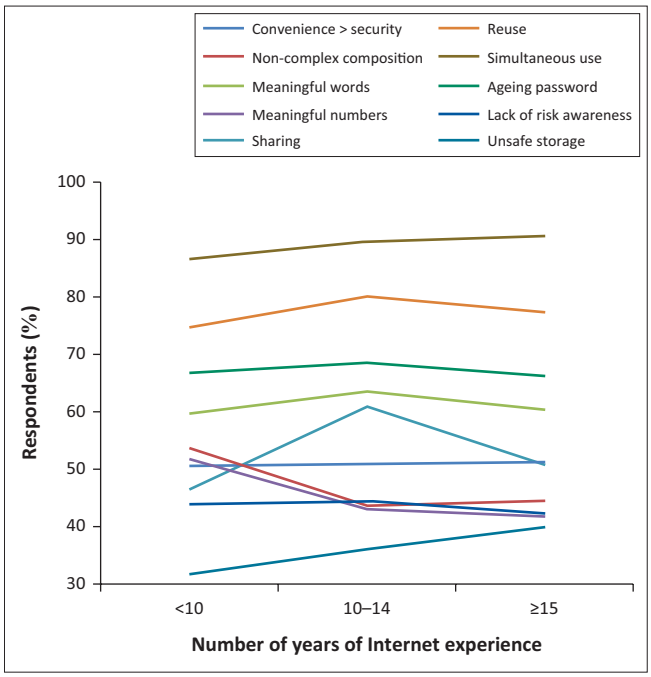

FIGURE 7: Weak password practices per years of Internet experience.

of regarding convenience as more important than security increased with education, the lack of risk awareness (i.e. not considering the risk associated with a password's use) when creating passwords seems to have decreased as levels of education increased. It is noticeable that password sharing was the highest among respondents with no formal after-school qualifications. Very interesting is the increase in unsafe storage with increased education levels.

Some of the variances could again only be properly explained once the cross-loading of factors, such as the higher age associated with higher levels of education or more sites accessed with higher levels of education, was investigated.

Internet experience

The weak practices analysed by years of Internet experience appear in Figure 7.

Years of Internet experience shows significant variance within the categories. Sharing of passwords, for example, peaks for the middle category (10–14 years Internet experience) and is significantly lower for both fewer and more years of Internet experience. It is possible that this trend could again be related to an increase in the numbers of sites accessed. Related poor practices of non-complex composition and meaningful numbers decrease with experience but, surprisingly, both unsafe storage and simultaneous use increased with the years of Internet experience.

Within-sample variation for different demographics

The variation within each demographic group was used to determine if a particular demographic group displayed a higher, or lower, prevalence for the particular measure. A confidence interval of 10% was selected for a medium focus. Where any demographic group displayed a prevalence of 5% higher than the mean, it is indicated as high and conversely a measure of 5% below the norm indicate a low focus. Figure 8 indicates the extent of the focus for the different improper password practices per demographic group.

From Figure 8 it is evident that areas of higher and lower focus exist within all the demographic groups, meaning that all demographic groups are in need of SETA. Furthermore it shows that the various demographic groups require tailored SETA programmes with different focus areas.

The results confirm that a one-size-fits-all approach for SETA programmes is not ideal. Although it could be argued that 'covering all bases' would be appropriate, relevance is a cornerstone for education and care should be taken to hide the specific knowledge required by an individual user, within a sea of non-relevant information that already shapes a user's behaviour.

However, there is also opportunity within this variance: the construct of social influence is well appreciated in the behavioural change and technology literature and allowing a natural transfer of good practices within diverse groups, although challenging, could have significant impact.

Conclusion

Although this study showed that there is a substantial incidence of poor password practices among South African computer users, research by Furnell and Esmael (2017) has shown that security-related information, guidance and feedback can positively influence secure behaviour. It has been argued that appropriate interventions can contribute to

Demographic	Category	Convenience > security	Non-complex composition	Meaningful words	Meaningful numbers	Sharing	Reuse	Simultaneous use	Ageing password	Lack risk awareness	Unsafe storage
Age group	< 35 years	M	M	M	M	H	M	M	M	H	H
	35–49 years	M	M	M	M	M	M	M	M	L	L
	50+ years	M	M	H	H	L	L	M	M	M	M
Gender	Male	M	M	L	L	L	H	M	L	M	M
	Female	M	M	M	H	H	M	M	H	M	M
Number of sites	< 10	M	M	M	H	L	L	M	M	M	H
	10—19	M	M	M	M	H	M	H	L	H	L
	20+	M	M	L	L	M	H	M	H	M	M
Highest level of education	School level up to Grade 12	L	M	L	L	H	M	M	M	H	L
	Graduated B degree/Diploma	M	M	H	M	M	M	M	M	M	M
	Post-graduate qualification	M	M	M	M	M	M	M	M	L	H
Years Internet experience	15+ years	M	H	M	H	L	M	M	M	M	L
	10–14 years	M	M	M	M	H	M	M	M	M	L
	< 10 years	M	M	M	M	M	M	M	M	M	M

L, low; M, medium; H, high.

FIGURE 8: Focus areas for security education, training and awareness programmes.

online security, even more so because the risks that users are exposed to are continuously changing.

Furnell (2008:9) warns that designers of SETA programmes must be wary of the 'build it and they will come' approach. It is essential that the relevant users, who need to hear the message, should be 'attracted' to the education message. This can only be achieved by using the most appropriate method of communication, which could be tailored for different demographic groups. Although the design of the message falls outside the scope of this research, it is important that appropriate messages for different demographic groups form part of SETA initiatives.

This article makes a contribution by showing the differences in overall poor password practices for South African online consumers (Figure 1), as well as per demographic group (Figure 8). The findings will allow for the design of targeted SETA initiatives to help create the security culture alluded to in the South African Cyber Security Policy Framework. A second contribution of this research is that it confirms that there are indeed differences between the different demographic groups, for certain password practices, and that one-size-fits-all SETA initiatives will not be appropriate.

However, it is not recommended that the differences displayed in this research be used as the basis for such design. Given the variations for different demographic groups, as well as the cross-loading effect between the groups, an appropriate SETA design should commence with individualised assessments of the recipient's current password practices. This research contributes by providing the set of practices that should be assessed to design individualised SETA for the individuals, or if required groups, who display particular poor password behaviour.

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

Each of the authors participated equally in the design of the survey instrument, the analysis of the results and findings and the writing of this article.

References

Adams, A. & Sasse, M.A., 1999, 'Users are not the enemy', *Communications of the ACM* 42(12), 40–46. https://doi.org/10.1145/322796.322806

Bonneau, J., Herley, C., Van Oorschot, P.C. & Stajano, F., 2015, 'Passwords and the evolution of imperfect authentication', *Communications of the ACM* 58(7), 78–87. https://doi.org/10.1145/2699390

Brostoff, S. & Sasse, M.A., 2002, 'Safe and sound: A safety-critical approach to security', in *Proceedings of the 2001 Workshop on New Security Paradigms*, Cloudcroft, NM, September 10–13, 2002, pp. 41–50.

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

Bryant, K. & Campbell, J., 2006, 'User behaviours associated with password security and management', *Australasian Journal of Information Systems* 14(1), 81–100. https://doi.org/10.3127/ajis.v14i1.9

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, United Kingdom, July 8–9, 2014, pp. 150–161.

Butler, R. & Butler, M.J., 2015, 'The password practices applied by South African online consumers: Perception versus reality', *South African Journal of Information Management* 17(1), 1–11. https://doi.org/10.4102/sajim.v17i1.638

Byrne, Z., Weidert, J., Liff, J., Horvath, M., Smith, C., Howe, A. et al., 2012, 'Perceptions of internet threats: Behavioral intent to click again', in *Proceedings of the 27th Annual Conference of the Society for Industrial and Organizational Psychology*, San Diego, CA, April 26–28, 2012.

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. https://doi.org/10.1080/10658980601051375

Carstens, D.S., McCauley-Bell, P.R., Malone, L.C. & DeMara, R.F., 2004, 'Evaluation of the human impact of password authentication practices on information security', *Informing Science Journal* 7, 67–85. https://doi.org/10.28945/503

Chandarman, R. & Van Niekerk, B., 2017, 'Students' cybersecurity awareness at a private tertiary educational institution', *The African Journal of Information and Communication (AJIC)* 20, 133–155. https://doi.org/10.23962/10539/23572

Chaudhary, S., Zhao, Y., Berki, E., Valtanen, J., Li, L., Helenius, M. et al., 2015, 'A cross-cultural and gender-based perspective for online security: Exploring knowledge, skills and attitudes of higher education students', *IADIS International Journal on WWW/Internet* 13(1), 57–71.

Chen, J., Paik, M. & McCabe, K., 2014, 'Exploring internet security perceptions and practices in Urban Ghana', in *Proceedings of Symposium on Usable Privacy and Security (SOUPS)*, Menlo Park, CA, July 9–11, 2014, pp. 129–142.

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*, Big Island, Hawaii, January 5–8, 2004, pp. 1–10.

Curry, M., Marshall, B., Crossler, R.E. & Correia, J., 2018, 'InfoSec Process Action Model (IPAM): Systematically addressing individual security behavior', *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* 49(1), 49–66.

Das, A., Bonneau, J., Caesar, M., Borisov, N. & Wang, X., 2014, 'The tangled web of password reuse', in *Proceedings of the Network & Distributed System Security Symposium* (NDSS), San Diego, CA, February 8–11, 2015, pp. 23–26.

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 8–12, 2007, pp. 657–666.

Fox, S., 2006, 'Are "wired seniors" sitting ducks?', *Pew Research Centre – Internet and Technology*, April 11, viewed 18 October 2017, from http://www.pewinternet.org/2006/04/11/are-wired-seniors-sitting-ducks/

Furnell, S.M., 2005, 'Authenticating ourselves: Will we ever escape the password?', *Network Security* 2005(3), 8–13. https://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. https://doi.org/10.1016/j.cose.2007.09.001

Furnell, S.M., 2008, 'End-user security culture: A lesson that will never be learnt?', *Computer Fraud and Security* 2008(4), 6–9. https://doi.org/10.1016/S1361-3723(08)70064-2

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(6), 529–539. https://doi.org/10.1016/S0167-4048(00)06027-2

Furnell, S. & Esmael, R., 2017, 'Evaluating the effect of guidance and feedback upon password compliance', *Computer Fraud & Security* 2017(1), 5–10. https://doi.org/10.1016/S1361-3723(17)30005-2

Garrison, C.P., 2008, 'An evaluation of passwords', *CPA Journal* May, 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, PA, July 12–14, 2006, pp. 44–55.

Gehringer, E.F., 2002, 'Choosing passwords: Security and human factors', in *Proceeding of the 2002 International Symposium on Technology and Society*, Raleigh, NC, June 6–8, pp. 369–373.

Ghazvini, A. & Shukur, Z., 2017, 'Review of information security guidelines for awareness training program in healthcare industry', in *Proceedings of the 6th International Conference on Electrical Engineering and Informatics (ICEEI)*, Langkawi, Malaysia, November 25–27, 2017, pp. 1–6.

Howe, A.E., Ray, I., Roberts, M., Urbanska, M. & Byrne, Z., 2012, 'The psychology of security for the home computer user', in *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, San Francisco, CA, May 20–23, 2012, pp. 209–223.

Huth, A., Orlando, M. & Pesante, L., 2012, *Password security, protection, and management*, United States Computer Emergency Readiness Team, Carnegie Mellon University, viewed 22 November 2016, from https://www.us-cert.gov/sites/default/files/publications/PasswordMgmt2012.pdf

Inglesant, P. & Sasse, M.A., 2010, 'The true cost of unusable password policies: Password use in the wild', in *Proceedings of SIGCHI Conference on Human Factors in Computing Systems*, Atlanta, GA, April 10–15, 2010, pp. 383–392.

ISACA, 2010, *IT standards, Guidelines and tools and techniques for audit and assurance and control professionals*, viewed 18 August 2016, from http://www.isaca.org/Education/Training/On-Site-Training/Documents/ALL-IT-Standards-Guidelines-and-Tools.pdf

Karlsson, F., Åström, J. & Karlsson, M., 2015, 'Information security culture – State-of-the art review between 2000 and 2013', *Information & Computer Security* 23(3), 246–285.

Kortjan, N. & Von Solms, R., 2014, 'A conceptual framework for cyber-security awareness and education in SA', *South African Computer Journal* 52, 29–41. https://doi.org/10.18489/sacj.v52i0.201

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, IL, April 21–22, 2015, pp. 13–22.

Kruck, S.E. & Teer, F.P., 2008, 'Computer security practices and perceptions of the next generation of corporate computer users', *International Journal of Information Security and Privacy* 2(1), 80–90. https://doi.org/10.4018/jisp.2008010105

Kruger, H., Steyn, T., Medlin, B.D. & Drevin, L., 2008, 'An empirical assessment of factors impeding effective password management', *Journal of Information Privacy and Security* 4(4), 45–59. https://doi.org/10.1080/2333696X.2008.10855851

McCloy, R.A., Campbell, J.P. & Cudeck, R., 1994, 'A confirmatory test of a model of performance determinants', *Journal of Applied Psychology* 79(4), 493–505. https://doi.org/10.1037/0021-9010.79.4.493

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. & Pattinson, M., 2017, 'Individual differences and information security awareness', *Computers in Human Behavior* 69, 151–156. https://doi.org/10.1016/j.chb.2016.11.065

McCrohan, K.F., Engel, K. & Harvey, J.M., 2010, 'Influence of awareness and training on cyber security', *Journal of Internet Commerce* 9, 23–41. https://doi.org/10.1080/15332861.2010.487415

McDowell, M., Hernan, S. & Rafail, J., 2013, *Choosing and protecting passwords*, United States Computer Emergency Readiness Team, viewed 21 April 2016, from https://www.us-cert.gov/ncas/tips/ST04-002

Michie, S. & Johnston, M., 2012, 'Theories and techniques of behaviour change: Developing a cumulative science of behaviour change', *Health Psychology Review* 6, 1–6. https://doi.org/10.1080/17437199.2012.654964

Milne, G.R., Labrecque, L.I. & Cromer, C., 2009, 'Toward an understanding of the online consumer's risky behavior and protection practices', *Journal of Consumer Affairs* 43(3), 449–473. https://doi.org/10.1111/j.1745-6606.2009.01148.x

Notoatmodjo, G. & Thomborson, C., 2009, 'Passwords and perceptions', in *Proceedings of the Australasian Information Security Conference (AISC2009)*, Wellington, New Zealand, January 20–21, Conferences in Research and Practice in Information Technology, vol. 98, pp. 71–78.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A. & Calic, D., 2015, 'Factors that influence information security behavior: An Australian web-based study', in *Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust*, Los Angeles, CA, August 2–7, 2015, pp. 231–241.

Redmiles, E.M., Kross, S. & Mazurek, M.L., 2016, 'How I learned to be secure: A census-representative survey of security advice sources and behavior', in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, October 24–28, 2016, pp. 666–677.

Riley, S., 2006, 'Password security: What users know and what they actually do', *Usability News* 8(1), 2833–2836.

Sasse, M.A., Brostoff, S. & Weirich, D., 2001, 'Transforming the "weakest link"- a human/computer interaction approach to usable and effective security', *BT Technology Journal* 19(3), 122–131. https://doi.org/10.1023/A:1011902718709

Shay, R., Komanduri, S., Kelley, P.G., Leon, P.G., Mazurek, M.L., Bauer, L. et al., 2010, 'Encountering stronger password requirements: User attitudes and behaviors', in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, Redmond, WA, July 14–16, 2010, p. 2.

Shen, C., Yu, T., Xu, H., Yang, G. & Guan, X., 2016, 'User practice in password security: An empirical study of real-life passwords in the wild', *Computers & Security* 61, 130–141.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. & Downs, J., 2010, 'Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions', in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Atlanta, GA, April 10–15, 2010, pp. 373–382.

Singleton, T.W., 2012, 'Evaluating access controls over data', *ISACA Journal* 1, 1–5.

Skinner, T., Taylor, J., Dale, J. & McAlaney, J., 2018, 'The development of intervention e-learning materials and implementation techniques for cyber-security behaviour change', in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Montreal, Canada, April 21–26, 2018, pp. 1–9.

Soomro, Z.A., Shah, M.H. & Ahmed, J., 2016, 'Information security management needs more holistic approach: A literature review', *International Journal of Information Management* 36(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

South Africa, 2015, *National cybersecurity policy framework for South Africa*, Government Gazette 39475:70, December 4 (Regulation Gazette No. 2561), Government Printing Works, Pretoria.

System Administration, Networking and Security Institute (SANS), 2014, *Password protection policy*, viewed 17 August 2016, from https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy

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. https://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. https://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.

Turan, M., Barker, E., Burr, W. & Chen, L., 2010, 'Recommendation for password-based key derivation – Special publication 800–132', *National Institute of Standards and Technology (NIST), US Department of Commerce, Computer Security Division, Information Technology Laboratory,* viewed September 2016, from http://csrc.nist.gov/publications/nistpubs/800-132/nist-sp800-132.pdf

Wash, R., Rader, E., Berman, R. & Wellmer, Z., 2016, 'Understanding password choices: How frequently entered passwords are re-used across websites', in *Proceedings of the Symposium on Usable Privacy and Security (SOUPS),* Denver, CO, June 22–24, 2016, pp. 175–188.

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

Zhang-Kennedy, L., Chiasson, S. & Van Oorschot, P., 2016, 'Revisiting password rules: Facilitating human management of passwords', in *Proceedings of the 2016 APWG Symposium on Electronic Crime Research (eCrime)*, Toronto, Canada, June 1–3, 2016, pp. 1–10.

Zviran, M. & Haga, W.J., 1999, 'Password security: An empirical study,' *Journal of Management Information Systems* 15(4), 161–185. https://doi.org/10.1080/07421222.1999.11518226