Towards online security: Key drivers of poor user behaviour and recommendations for appropriate interventions

M.J. Butler*
University of Stellenbosch Business School, P O Box 610, Bellville, 7535, South Africa

*To whom all correspondence should be addressed
martin.butler@usb.ac.za

Online commerce has grown significantly and securing this channel of commerce is of vital importance for organisations. In the quest to secure the online world, users are often referred to as the weakest link in online security since their behaviour could impact negatively on systems security. User education and awareness programmes to develop and enhance the required skills and appropriate frame of mind are common approaches to improve online security.

Focussing on the drivers of change in user's online security behaviour can assist in defining appropriate interventions. Key human behaviour models where used to define these drivers. The drivers of change in online security behaviour was used to design an instrument used to survey South African online consumers to determine the prevalence, or not, of factors that determine secure or unsecure behaviour.

The data from the survey was analysed to highlight the Knowledge, Capability and Motivation to behave in a secure manner, as well as test for potential aspects that have influenced past behaviour and that could potentially influence future behaviour. Based on the determinants of behaviour, as well as identified deficiencies in password behaviour as identified by the survey, a list of potential considerations for the designers of IS security interventions is presented.

Introduction

Securing information systems

Ensuring that information is only made available to or disclosed to authorised individuals, entities, systems or processes forms part of information security. User identification and authentication, through systems such as passwords, remains the most common method used to control access and ensure confidentiality and availability (Furnell, Dowland, Illingworth & Reynolds, 2000:529) and remains central to information security.

Zviran and Haga (1999:164) remark that almost every penetration of a computer system at some stage relies on the attacker's ability to compromise a password. Attacks to hack, crack or discover passwords, which in turn can be used to gain unauthorised access to accounts and systems, are common. After initially addressing the passwords vulnerability challenge with more complex technology, researchers began to acknowledge that Information Systems (IS) security involves both people and technology (Sasse, Brostoff & Weirich, 2001:122).

A lack of knowledge among users was identified by Kortjan and Von Solms (2014:1) as a factor that contributes to unsafe password behaviour. If users do not apply proper practices when selecting and safeguarding passwords, those passwords are more vulnerable, which directly affect computer security (Gehringer, 2002:369). The actions of users that weakens online security through poor password practices, led researchers to refer to the users as the 'weakest link' in the information security chain (Tam, Glassman & Vandenwauver, 2010:233; Notoatmodjo & Thomborson, 2009:71).

After researchers initially suggested security education, training and awareness programs to improve password performance among computer users (Conklin, Dietrich & Walz, 2004:5), Pfleeger and Caputo (2012) highlighted the need for a greater understanding of the password behaviour of users when designing these programs to prevent them from being the weak link in systems security. Charoen, Raman and Olfman (2008:69) described how the appropriate interventions could have a positive effect on user behaviour. Through a set of tailored action research interventions they were able to "…improve system users' behavior related to passwords" (Charoen *et al.*, 2008:55).

However, referring to online users as the weakest link is flawed. It is the point of departure of this paper that the user's behaviour, instead of the user, represents the weakest link in information security. This subtle yet important distinction shifts the emphasis for securing systems from the user, representing the problem that needs to be addressed, to the user's behaviour that can, and should, be (positively) influenced to improve online security.

Research problem and objective

Although researchers suggest a greater understanding of the behaviour of users, it is not evident from the literature whether existing security and awareness programs focus on the appropriate aspects of human behaviour, indicating that the design of these programmes leave a lot to be desired. In fact Leach (2003:685) believes that … "security awareness programmes often seem more likely to put users to sleep than to improve their behaviour". It is therefore necessary to design programmes that address the factors that shape users' behaviour and also ensure that these programmes keep users engaged.

Sasse, Brostoff and Weirich (2001:122) recommend that system designers identify the underlying causes for poor user behaviour and address these issues to improve computer security. Research has shown a 'strong and consistent' as well as a theoretically grounded relationship between users' intentions and actual behaviour (Anderson & Agarwal, 2010:614). In order to shift the emphasis from the user to the user's behaviour it is important to review current theoretical constructs which deal with user behaviour, or the then user's intent to behave, to establish the factors that influence human behaviour. By shifting the emphasis to the determinants of secure password behaviour, the common mitigation measure of 'education and awareness' can be optimally directed at the areas that could have the greatest effect on the user's behaviour for the effort exerted.

The purpose of this study is to:

1. Review potential theories in human behaviour that could assist in developing sustainable intervention to improve online security.
2. Develop an instrument to survey online consumers to determine their relative performance in factors that affect password behaviour.
3. Analyse respondents' measured and reported password practices to assist practitioners to design appropriate measures to improve password performance.

Literature Review

Information system security and user behaviour

Information security includes three main dimensions: confidentiality, availability and integrity (ISO/IEC, 2014:13). One of the aims of information security is to ensure that information is only made available to or disclosed to authorised individuals, entities, systems or processes. This can be achieved through the implementation of suitable access controls, such as password systems, which identify and authenticate users to prevent unauthorised access. Passwords remain a commonly used, cost effective and efficient method to identify and authenticate computer users (Campbell, Kleeman & Ma, 2007:2).

Stallings (1995:213) describes the use of a password system as "the front line of defence against intruders". The principle behind password-based security is that an authorized computer user selects and remembers a secret (the password) and that this secret in turn is used to identify and authenticate the identity of the authorized when access is requested (Conklin *et al.*, 2004:1). Due to the role that the user plays in ensuring the effectiveness of a password-security system and the risks and consequences associated with the improper selection and use of passwords, it is essential that all users understand the risks associated with the use of IS, including the consequences of applying improper practices (Kritzinger & Von Solms, 2010:840).

The first step in a password-based authentication system is that users select passwords that are 'strong', yet memorable (Conklin *et al.*, 2004:5). However, users rarely choose passwords that are both hard to guess and easy to remember as they are confronted with a 'security-convenience trade-off' (Tam *et al.*, 2010:242) in spite of users' knowledge of proper password practices (Weber, Guster, Safanov & Schmidt, 2008:46). A possible reason can be that the users suffer from 'password overload' which Notoatmodjo and Thomborson (2009:71) identified as a major contributor to unsafe password practices. In addition, users often perceive security measures as 'obstacles' and secondary to the primary task that they are trying to achieve, resulting in users who 'ignore or even subvert the security' (Pfleeger & Caputo, 2012:602). Even the most sophisticated security systems are rendered vulnerable if computer users do not choose and manage their passwords properly (Tam *et al.*, 2010:233).

Authors have also commented on the importance of a security culture within organisations and the interdependency of awareness programmes and a culture of security. According to Drevin, Kruger and Steyn (2007:36), a "strong ICT security culture cannot develop and grow in a company without awareness programmes". Their work emphasized the importance of users accepting responsibility for actions performed. Da Veiga and Eloff (2010:196) designed an assessment instrument to measure the maturity of this IS security culture within an organisation. Van Niekerk and Von Solms (2010:476) stated that it "has become widely accepted that the establishment of an organizational sub-culture of information security is *key* to managing the human factors involved in information security".

According to Pfleeger and Caputo (2012:597) a key element to improve security is "acknowledging the importance of human behaviour when designing, building and using cyber security technology". When the usability (from a user perspective) is neglected by designers of technology, it leads to increased pressure on the users to enforce security (Brostoff & Sasse, 2002:41). Researchers (Furnell, Jusoh & Katsabas, 2006:27; Furnell, Bryant & Phippen, 2007:416) recommend improving the usability of security features as users often don't apply these features because they have problems to find, understand and use these security features. Inglesant and Sasse (2010) advise greater emphasis on human computer interface (HCI) principles to increase the usefulness and effectiveness of password security.

Theoretical frameworks of human behaviour

Although commonly used theories in IS such as the Technology Acceptance Model (TAM), Diffusion of Innovation (DOI), Information Processing Theory (IPT) and the Delone and McLean's IS success model were reviewed, they did not contribute directly towards the research objective. The theoretical constructs presented in this section are less common, although not completely absent, in IS research, but were found to be more applicable towards designing interventions that shape human behaviour, and ultimately improve online security.

Socio-technical Theory

The Socio-technical Theory (STT) was born out of research conducted into implementation problems experienced with the introduction of technology which is often met with resistance by users and as a result fail to achieve the expected benefits. STT researchers, mainly from behavioural sciences, suggest that a fit between the technical sub-system and the social subsystem is required. The technical subsystem comprises the devices, tools and techniques, while the social subsystem comprises the employees and the knowledge, skills, attitudes, values and needs they bring to the work environment, as well as the reward system and authority structures that exist within the organization (Davis, Challenger, Jayewardene & Clegg, 2014:172).

One of the first applications of the STT principles in IS was the work of Bostrom and Heinen (1977:11-28) that provided new insights on management information systems problems and failures. An IS development methodology on socio-technical principles, called ETHICS, was also designed by Mumford (1995). Clegg's work brought STT into the online domain by outlining the way in which socio-technical principles can be implemented to encompass the impact of the internet (Clegg, 2000). Although not as omnipresent as some of the more well-known IS theories, STT seems to enjoy growth in the IS security domain where discourse concerning the HCI remains active.

The cornerstone of the socio-technical approach is that a fit should be achieved by a design process aiming at the joint optimisation of the subsystems, i.e. any organisational system will maximise performance only if the interdependency of subsystems is explicitly recognised. Hence any designer must seek out the impact each subsystem has on the other and aim to achieve superior results by ensuring that all the subsystems are working in harmony (Cherns, 1976 as cited by Davis *et al.*, 2014:173). This principle is well-established in the IS security domain where the TAM, for example, includes '*Ease of Use*' as a key attribute towards technology adoption, as well as in IS security research where the duality of the system's controls and the user's ability determine the attained level of security.

Theory of Planned Behaviour

The Theory of Planned Behaviour (TPB) is a popular theoretical model used to deal with user behaviour, or rather the intent to behave in a particular manner (Ajzen, 1991). The premises of the TPB, namely that there are different aspects that influence behaviour (in this instance password performance), finds substantive support in the literature.

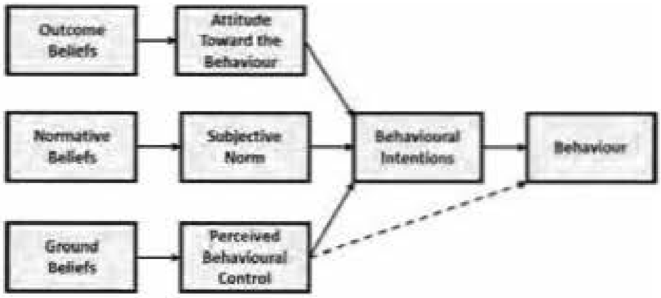

Figure 1: Theory of Planned Behaviour
Source: Ajzen (1991)

The TPB suggests that the intention to perform different behaviours can be predicted from *Attitudes towards behaviour*, *Subjective norms* and *Perceived behavioural control* (refer Figure 1). According to Ajzen (1991) these intentions account for a considerable amount of variance in the actual behaviour. After recent calls (Sniehotta, Presseau & Araújo-Soares, 2014:1-7) for the TPB to be rejected by the academic community, Ajzen (2014) supplied an excellent rebuttal pointing to the massive contribution of research using the TPB over more than two decades. The TPB have been used extensively in IS research to study information security policy compliance (Burcu, Cavusoglu & Benbasat, 2010:523-548), privacy in the digital age (Bélanger & Crossler, 2011:1017) and predicting the adoption of online procurement adoption (Aboelmaged, 2010:392).

Although these beliefs all influence the intention to perform certain actions (behaviours), the large majority of the existing literature in the IS field, such as many studies on the technology acceptance model (TAM), has focused mostly on investigating attitude and its antecedents (behavioural beliefs) because these beliefs can be reshaped by external interventions (in the form of objective information concerning information technologies and their design) to influence those behavioural beliefs and, in turn, improve attitude toward behaviour (Wixom & Todd, 2005).

The focus on *Attitude towards behaviour* is significant in the context of this study since the user's outcome believe largely shapes their attitude towards their password selection and management. Whether a user feels secure or are concerned about a possible security breach, would largely shape their behaviour (negatively). The risk or value associated with the site being visited also plays a role in attitude, as well as the users' perception of potential positive or negative consequences associated with their action.

Subjective norms are what the user believes how others would view their behaviour. Selecting and managing a password is not done in a social context and very rarely sees any social interaction. This has, potentially, a rather low impact on user behaviour for online authentication since the authentication is not observed by other stakeholders. However, this could be changed by educational interventions. A mere discussion between users of varying levels of security awareness, rather than the facilitator's attempt to increase knowledge, could impact the subjective norms and shape user behaviour.

Perceived behavioural control stems from self-efficacy theory and describes a person's judgment about being able to perform a particular activity - the 'I can' or 'I cannot' belief. Unlike self-esteem, which reflects self-worth or value, self-efficacy reflects how confident an individual is about performing specific tasks. It can be seen as the ability to persist or a person's ability to succeed with a task. With online passwords past successes or failures in meeting system enforced complexity measures could dramatically impact a user's current behaviour. By creating interventions that allow users to build their 'I can' belief in creating strong passwords, or even remembering strong passwords, the user's behaviour could be positively influenced over time.

Although the TPB is not necessarily appropriate to determine the behavioural performance it is valuable to use as a model to design interventions to improve password performance. According to Hardeman, Johnston, Johnston, Bonetti, Wareham and Kinmonth (2002:123) the TPB have potential for developing behavioural change interventions. Their research reviewed studies applying the TPB to behavioural change interventions and identified 24 distinct interventions, of which two-thirds were effective in changing behaviour. However, evidence supporting mediation by TPB components (Figure 1) was sparse.

The Rational Choice Theory

Rational Choice Theory (RCT) is a neo-classical economic approach that offers an explanation for decisions made by individuals when faced with choices. According to RCT individuals determine how they will act by balancing the costs and benefits of the options presented (Dowding, 2010). Because of its parsimonious explanation the RCT has been widely used to study individual, social and economic behaviours in various contexts, including IS (Li, Zhang & Sarathy, 2010; Vance & Siponen, 2012).

In rational decision making, an individual first recognizes alternative courses of action (Paternoster & Pogarsky, 2009) and then contemplates the likely outcomes of each course of action. Outcomes refer to states of the system after an action is taken. The work of Tam *et al.* (2010:235) elaborates on the *Convenience versus Security* trade-off and provides a clear application of the RCT in shaping the behaviour of online users. Although models used in RCT are diverse, all assume that individuals choose the best action according to personal utility and outcome believes. Proponents of rational choice models do not claim that a model's assumptions are a full description of reality, only that good or bad models can aid reasoning and assist in formulating falsifiable hypothesis, whether intuitive or not.

The RCT provides some guidance in terms of measuring secure behaviour, since the rational process of selecting the outcome that maximizes personal advantage could be used in an instrument to test whether users correctly identify the option that maximizes personal advantage, for example to distinguish between different password options presented and asked to select the most secure (best) password. Secondly, in defining appropriate actions it is important to focus on the user's personal value maximization, that is, the framing of the outcome should be addressed and lasting interventions will shape the state of the possible outcomes as a mechanism to change behaviour.

Heider's determinants of performance

McCloy, Campbell and Cudeck (1994:493) stated that users differ in their password performance as their behaviour is influenced by a number of aspects. According to Heider (1958) an individual's performance in a particular task is a function of the individual's ability and motivation relating to that task:

Performance = Ability x Motivation

Ability refers to the knowledge, skills and competencies that enable a human to perform a particular task. It is associated with what people know and think, what they can do and how they behave because of how they feel. Aspects that can influence a user's ability include their personality, prior education as well as previous experience (Anderson & Butzin, 1974:598). According to Anderson and Butzin (1974:599) *Motivation* refers to the underlying drive behind a user's particular behaviour in performing that task. The user's desire to extend effort, the intensity of the effort, as well as the commitment in extending effort, all impact motivation.

Clearly both the *Ability* and *Motivation* dimension of Heider's function is aligned with perceived behavioural control, or self-efficacy. Although there is a degree of alignment between TPB and Heider's model they serve different purposes. The TPB is aimed at listing factors that impact potential behaviour, whereas Heider's model is concerned with performance, i.e. displayed behaviour. In line with the objective of the research the concept of displayed behaviour, as per Heider's model, is used for further dissection.

McCloy's function for performance

McCloy *et al.* (1994) extended Heider's work by further refining the concept of *Ability*, taking cognisance of the difference between *know-how* and *displaying know-how* through application. According to McCloy *et al. Ability* can be divided into declarative knowledge (DK) (a function of the knowledge of facts, rules, principles and procedures relating to a task); and procedural knowledge and skill (PKS) (the capability when DK is successfully combined with knowing how and being able to perform that task). Heider's function for performance was thus refined as consisting of **Declarative knowledge (DK), Procedural knowledge and skill (PKS)** and **Motivation (M)**:

Performance = f (DK, PKS, M)

It is not the objective of this research to determine the moderating effect of each of these aspects on password performance, but rather to determine if there are measurable deficiencies in each of these components among users and then to define appropriate interventions to address this to improve the password performance.

Password performance model

It was decided to use the above function for performance to design an instrument that can test users' levels within each of the three areas that can have the potential to impact password performance. Three determinants of a user's password performance were defined:

- **Knowledge (K)**: the user's knowledge and education relating to password practices;
- **Capability (C)**: the user's competence to successfully combine password-related knowledge with knowing how and being able to apply proper password practices;
- **Motivation (M)**: the underlying desire behind the user's password behaviour.

This construct for the determinants of password performance represents an opportunity to deconstruct poor password performance in a way different to most research to date. If the reasons why users do not apply proper password practices are known, then appropriate methods aimed at addressing the underlying causes for poor password behaviour can be designed and implemented to improve password security.

In addition to testing the attributes that impact behaviour through this study an opportunity also existed to gather information about factors that lead to past changes in behaviour as well as potential future behaviour changes among users. These factors were used to determine **Drivers for change (D)** and can be used to determine if the password performance model indeed describes the drivers of change by correlating the factors that lead to behavioural change to *Knowledge*, *Capability* and *Motivation*.

Research Methodology

Research Design

A survey was used to determine users' current performance in each of the three key areas of password performance. Survey designs are appropriate when researching behaviour. A survey consists of a predetermined set of questions that is given to a representative(s) of the larger population of interest (Shaughnessy, Zechmeister & Jeanne, 2011). The survey designed also used an online platform, when given the nature of what is being researched (behaviour of online users), was deemed appropriate for this study.

Research instrument

A new research instrument was created for the survey that tested four different elements:

- Knowledge (K);
- Capability (C);
- Motivation to behave securely (M);
- Self-reported drivers of change (D).

The respondents' **Knowledge** (K) was tested in the questionnaire by means of a set of questions that tested their 'know-what' of strong and secure passwords as well as good management practices in terms of safekeeping and regularly changing passwords.

The respondents' **Capability** (C) was tested by asking them to rank different combinations of passwords from the most to the least secure, testing 'know-how'. In ranking the passwords they displayed their ability to understand and combine factors such as password length, complexity, different character sets, as well as common words. Respondents were also asked about the sharing of passwords and when they last changed their passwords to obtain an indication of practice, i.e. knowing about regular changes constitute *Knowledge*, having changed the password in the last 12 months constitutes *Capability*.

It is acknowledged that research in the field of **Motivation** (M) is highly complex and best left to experienced researchers in this domain. However, a simple well-known trade-off in terms of security and convenience when users choose and manage passwords provided a good indication of their underlying motivation. Respondents were tested about prioritising security and it was decided that security as a top priority is an acceptable predictor of **motivation to behave securely**. A set of questions probed users' propensity to behave either with convenience or security as the most important factor.

As **Drivers of change** (D) respondents were asked to select from past experiences that have led to a change in password (reality) and potential future events that will lead to changes (reported perception). Respondents were also provided with an optional open-ended question prompting for other triggers that will potentially drive a change in password behaviour.

The survey contained 43 questions, both structured and open-ended. It was designed and refined via two iterations of pilot testing with a group selected to range from computer novices to online experts. Users validating the survey were asked to highlight any questions that forced answers and also indicate an ambiguity in the question set. A third round of testing revealed no issues with the question set after incorporating all user feedback.

Data gathering and analysis

The survey was distributed via email to a database of online South African users from the author's tertiary institution. This distribution list consisted of just below 10 000 email addresses on the graduate school's contact list. It was also distributed via snowball method by the researcher specifically, targeting the underrepresented areas of younger (pre-employment) and older (post-employment) internet users. A review of the survey demographics revealed a slight bias in terms of educational levels when compared with the online population, but no significant bias in terms of age and gender distribution.

In order to put users who might fear that they may be required to share potentially sensitive information at ease, care was taken to ensure respondents that their passwords would not be asked, and that the purpose of the study was to merely gather information on the practices that users apply, not passwords.

Users' perceptions about their password practices' knowledge and application as well as motivation were analysed using descriptive statistics. Based on the responses a measured ability for the respondents' *Knowledge*, *Capability* and *Motivation* was calculated. A textual analysis of the open-ended questions was done by coding the text with recurring themes that emerged from the answers.

Sample size and response rate

For a population of >1mil (SA internet users) and a confidence interval of 99% a sample population of at least 384 responses is required. Although no inferential statistics will be used, the sample population indeed met this minimum criterion. There were a total 794 responses to the survey, but as only respondents that use online banking was included in the final sample, the dataset consisted of 737 valid and complete responses.

Limitations of the research

It is acknowledged by the author that certain limitations exist due to the methods employed. The distribution of the email to the graduate school's database and personal contacts do present and element of **bias**. Although comparisons with the general online population only indicated an element of bias in terms of educational levels, it is not an ideal sample.

Due to the definition of *Knowledge* (*Know what*) and *Capability* (*Know how*) there is a **moderating effect of *Knowledge* on *Capability***. It is rather difficult to apply without knowing and it is to be expected that a large degree of the variation in capability could be explained by the variation in knowledge.

The challenge of **reported versus actual behaviour** is well documented in survey research. The value of data depends upon how truthful respondents are in their answers and since they know that their responses are being recorded and analysed, they may feel pressured to respond to questions in a certain way, the so-called social desirability. The survey design took cognisance of this by ensuring anonymity and requesting that respondents indicate current and past behaviour, irrespective of their view on the desirability, or not, of said behaviour.

Data Analyses and Results

Knowledge, capability and motivation

The responses were analysed to determine the levels of *Knowledge*, *Capability* and *Motivation*, independently for each respondent. Figure 2 provides a frequency distribution of the analyses.

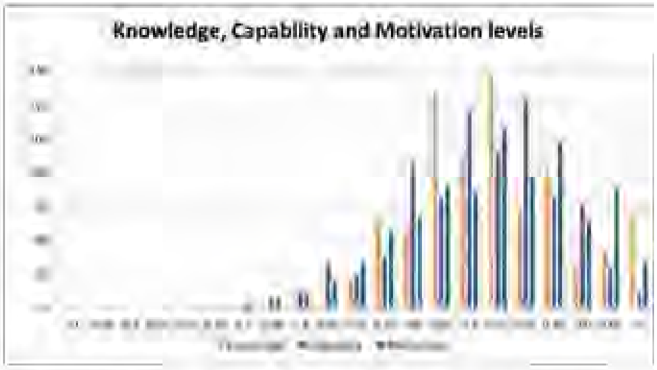

Figure 2: Knowledge, capability and motivation of respondents

When analysing the *Knowledge* of the 737 respondents, 55 respondents (7,5%) perceived that they possess absolute knowledge of password practices. However, a mere 9 respondents (1,2%) demonstrated flawless *Capability* to apply proper password practices. Only 27 (3,7%) displayed a perfect 'security first' aptitude when selecting and managing passwords indicating perfect security conscious *Motivation*.

Table 1 indicates the average measured ability for all three attributes of the password performance model as well as the standard deviation.

Table 1: Respondent performance variation (n = 737)

Attribute	Knowledge	Capability	Motivation
Mean	0.69	0.72	0.71
Standard deviation (σ)	0.136	0.136	0.152

Although the means for *Knowledge* and *Capability* are slightly different, the variations are the same, lending some support for the potential moderation effect of *Knowledge* on *Capability*.

The good, the bad and the ugly

The analysis suggests that all three factors (*Knowledge, Capability* and *Motivation*) contribute to poor password practices among South African online consumers. For further analysis levels of proficiency in each of these domains were defined as indicated below:

- Excellent: Higher than 80%;
- Good: Between 65% and 80%;
- Average: Between 50% and 64%;
- Poor: Less than 50%.

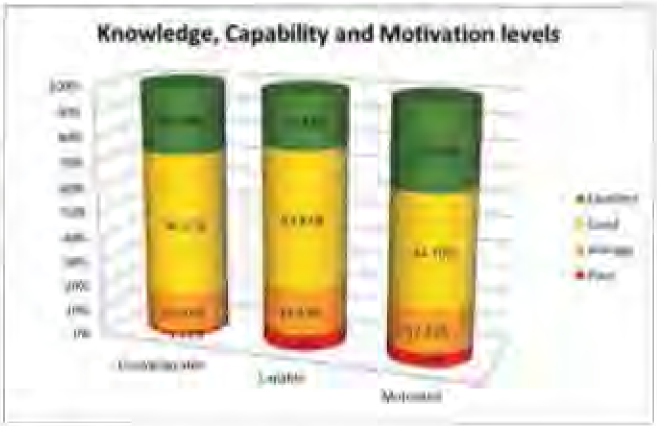

Figure 3: Categorised performance

The analysis of the responses in these different criteria is shown in Figure 3. More users (33.4% as opposed to 21.4% and 26.6%) are classified as being well-motivated using the defined bins. However, it is evident from Table 1 that there is a higher variance in Motivation ($\sigma = 0.152$) than either Knowledge or Capability. A higher variation could indicate a potential to (positively) influence the Motivation to behave securely.

The analysis indicates the presence of all three factors contributing to poor password behaviour amongst the respondents. Although the *Motivation* levels are slightly better than those for *Knowledge* and *Capability*, all three factors remain problematic and are thus drivers of poor password performance among South African online consumers.

Drivers of change

It is evident from the responses that there are certain past and future experiences that affect certain users' motivation to improve password practices. Responses about past experiences that will trigger a positive (more secure) behavioural change are provided in Table 2. The question was phrased specifically to ask about a password change (measurable) rather than a more desirable behavioural change, since that would constitute a perceived change.

Table 2: Past experiences that triggered a change

Event	Resulted in change	Did not result in change	Positive change in
Learned that my current password was not very secure (*n* 205)	47.3%	52.7%	Knowledge & Capability
Am aware of the need to regularly change my password (*n* 501)	32.9%	67.1%	Knowledge & Capability
Have personally suffered a security breach (*n* 93)	87.1%	12.9%	Motivation
Learned about bad experiences from friends, family or colleagues (*n* 285)	30.9%	69.1%	Motivation
Became aware of security breaches in the media (*n* 485)	25.1%	74.9%	Motivation

Of particular interest in the responses about **drivers of change** is:

- The poor reaction (67.1% no action) related to the need to regularly change passwords;
- The 12.9% of users that do not change passwords even after suffering a security breach;
- The low impact of media (74.9% no action) and even friends, colleagues and family (69.1% no action) in motivating users to change passwords. Sharing tales of pain may be less effective than what is commonly believed.

Respondents were also asked via an open-ended question to share past instances that lead to changes in passwords. These were dominated by forced changes such as "*entered wrong three times*" (Respondent 103), "*lost card and renewed PIN and Password*" (Respondent 443) and similar events. One response, however, clearly stood out. According to Respondent 248 "*the responsibility to ensure the safe usage of internet banking is on the bank not on me. If my account gets hacked, for whatever reason, they are insured against it.*" This indicates a clear abdication of responsibility towards the institution and a lack of awareness of the shared responsibility for security, an aspect to be emphasized during awareness training.

Table 3 contains users' perceptions about future events that may trigger a change in passwords.

Table 3: Future experiences that may potentially trigger password change

Event	Will not lead to change	May lead to change	Will definitely change
When hearing about financial losses in the media	17.8%	63.9%	18.3%
When hearing about financial losses suffered by people I know	13.6%	59.2%	27.2%
Suffering personal losses	1.9%	5.5%	92.6%
When requested by my service provider	4.3%	19.1%	76.6%
When I know my details have been compromised	0.9%	3.0%	96.1%
Realising that I re-use my internet banking password on other internet sites	11.4%	35.1%	53.4%
Realising that my current password is not very secure	4.7%	29.3%	65.9%

When prompted about other future events that could potentially trigger a password change, three categories of responses stood out:

- An increase in knowledge as is evident by the response "*A better understanding of the risks involved in breaking my passwords*" (Respondent 19) occurred in 5% of respondents;
- Merely completing the survey created an increased awareness and "*this survey*" (or similar) was indicated by 17% of respondents, some even indicating that they will immediately change their passwords after completing the survey;
- A personal security breach. With the exception of one instance of mentioning the media by Respondent 513, the only other option already provided in this question was a personal security breach.

The survey achieved an unintended objective, namely imparting knowledge (according to respondents), as is evidenced by Respondent 527's statement "*I didn't realize that using the same password for different unrelated websites is a security risk. However, I will get unique passwords/pins now!*" The following also emerged from the analysis of the text:

- **Sharing of passwords**: Passwords are shared with spouses, with some respondents indicating that divorce will be a reason to change passwords.
- **Password fatigue** is clearly a concern for respondents with Respondent 137 indicating that "*It is impossible to use passwords safely - there simply are too many for any human brain to remember without writing it down. And you have to remember the Pin, the username and the password!*"
- **Lack of responsibility**: Elements of lack of responsibility was evidenced with a response like "*This survey is driving home the fact that I might want to change my password from time to time - HOWEVER, if it aint broken why fix it?*" (Respondent 41).

Findings and discussion

Knowledge as a driver of behavioural change

Furnell (2007:445) remarks that one of the reasons why many computer users do not apply safe password practices is because "they may not know any better" due to a lack of appropriate knowledge, guidance and support. This may lead to users applying unsafe practices without them even being aware of this.

The survey confirmed that knowledge among users is indeed lacking. Nonetheless analysis of the open-ended questions clearly displayed the (positive) unintended initiation of a change in behaviour due to the knowledge (and motivation). A final question asked respondents to indicate if they want to receive guidelines on safer password practices to which 73.2% responded positively, indicating a willingness to receive relevant new knowledge. Increasing knowledge about what constitutes a strong password is not a new concept in IS security interventions, far from it. However, the study confirms firstly a lack of knowledge and secondly the positive impact of imparting new knowledge. It is important that knowledge is not dumped in a one-size-fits-all method. Engaging users in the process and providing users with relevant knowledge based on the attributes of their own passwords, rather than merely stating generic information, is important. Appropriate interventions obtain user engagement, is tailored to work with the users' current levels of knowledge and protect their privacy (which remains a challenge when personalizing IS security education).

In addition, it is important that users' awareness be maintained over time. While advising against punishing users for poor password behaviour, if security is compromised and no action is taken, users may be prone to be less security motivated as they feel that security 'does not matter anyway'. Conversely, if the system and security measures seem invincible, users may tend to be more careless, since they perceive the security threat to be low.

Capability as a driver of behavioural change

Tam *et al.* (2010) stated that although users possess the required knowledge, their practical application thereof often lacks, indicating an inability to apply the knowledge, i.e. they may have the 'know-what' but lack the 'know-how'. Nine questions in the survey required respondents to assess the strength of various passwords. Only 11% of respondents were able to rank the strength of all passwords correctly. When compared with the 35% of respondents who indicated that they 'knew exactly' what a strong password was, it is clear that users may not be capable to apply their knowledge on password practices.

Possible reasons for respondents' incapability to apply proper password practices may be that users overestimate their perceived knowledge regarding password practices due to a phenomenon known as optimistic bias (Weinstein, 1980:806). Optimistic bias may lead password users to overestimate their ability to create 'strong' passwords that are properly managed and protected. It is thus important that the application of good practice forms part of the password education process when designing security improvement interventions. Websites such as *howsecureismypassword.org* and *www.passwordmeter.com* can assist to determine password strength and provide real-time feedback by showing characteristics of good and poor passwords. Adams and Sasse (1999:44) recommend including online constructive feedback during the password construction process as a means in increase 'know-how'.

The gamification of security practices presents another opportunity to improve knowledge, grow capability and get learner engagement. Thornton and Francia (2014) have shown how gamification of IS security can have a positive effect on user engagement and succeed in improving their capabilities. Gamification is of course not without perils and a meta-study by Hamari, Koivisto and Sarsa (2014) of previous work provides guidance on the appropriate design of these interventions. Importantly, gamification turns knowledge into capability through practical application of the principles. In addition, it could also show deficiencies in knowledge of which users may not be aware.

Motivation as a driver of behavioural change

An important factor that impacts negatively on motivation is the vast amount of password-protected systems. This is confirmed in the survey where 16.3% of respondents indicated that they need to authenticate themselves at 20 or more systems online. These multiple places of authentication, coupled with policies that impose regular changes in passwords, clearly intensify the strain on users' memories. Carstens, McCauley-Bell, Malone and DeMara (2004:68) have commented on the increasing number of password-protected systems, enforced password lifetimes and composition rules and the challenges that it provides for human memory - the 'password overload' (Notoatmodjo & Thomborson, 2009:71).

Interventions aimed to motivate a user to act more securely need to take cognisance of this password overload. Sharing best practices and composition rules with users could in fact decrease the motivation to behave in a secure manner. When the security motivation is secondary to convenience it leads to weak password practices, which include using short and weak passwords that are easy to remember, sharing passwords, writing down passwords, re-using passwords and not changing passwords regularly (Yan, Blackwell, Anderson & Grant, 2004:25). When interventions have value, rather than threatening compliance, they may be more sustainable, in line with respondent 93 that stated "*If something new and convenient comes up, I will certainly try it.*"

Recommendations

To improve password performance one of the most common suggestions made by researchers is the education of computer users through improved security education, training and awareness programs (Furnell *et al.*, 2007:417). It is important that initiatives to improve the IS security culture via education and awareness interventions focus on the underlying determinants of poor password performance evident from this study. The literature confirms that training programs do not necessarily address all the issues that should be dealt with (Anderson & Agarwal, 2010:614). Table 4 contains a summary of the recommendations that flow from the analysis performed.

Table 4: Recommendation to improve Knowledge, Capability and Motivational levels

Addresses	Recommendations
Knowledge	Design interaction discussions to allow peer-to-peer sharing of best practices rather than an expert instructing users about best practice.
	Create opportunities that show users how to remember strong passwords via known techniques as well as acceptable technologies.
	Shared responsibility is fundamental to IS security maturity. Design interventions to allow the expression of counter arguments and allow ample time to discuss and dissect this option. Use analogies like the shared responsibility of the vehicle manufacturer and the driver of the vehicle to ensure safe roads.
	Use forced change interventions as an opportunity to improve behaviour. It is evident from the responses that passwords are changed when enforced by systems, explain the positive value in using it as an opportunity to improve security.
Capability	Create opportunities that allow users to build their 'I can' do belief in creating strong passwords by practicing their know-how in a simulated environment.
	Use the omnipresent challenge of password fatigue to make an emotional connection by stating that it is a reality and will only get worse. Show users how well-documented techniques and available technology could assist with the challenge.
	Users have to apply new knowledge ('know-what') in a safe environment and be given feedback to both create 'know-how' and enhance self-efficacy.
Motivation	Design interventions around the principle that maximum personal advantage is also the greater advantage – a positive outcome for all. Do not fight the RCT principles, rather design learning that use it.
	Use the security-convenience trade-off as an opportunity, not a threat, by showing techniques and technologies that are more convenient and more secure than committing to memory.
	Do not threaten users with compliance - where absolutely necessary this can be system enforced. Rather use the concept of us (user and organisation) versus them (cyber criminals), it should never be the user's convenience versus the organisation's policies.
	Use gamification, where possible, to make the sessions more interactive and engaging. A simple prize for the strongest password on howstrongismypassword.org could be a fun learning experience.

The recommendations (Table 4) are at different levels of granularity and encompass principles like intervention design, facilitation style and education techniques. It is not intended to be a complete set of guidelines but merely a supplementary set of principles that could be used by practitioners and designers of security awareness interventions in their strive towards a secure IS environment. Future research could potentially focus on determining the value of these concepts in improving online security.

Conclusion

The value of educational programmes in improving online security was confirmed by the work of Bauer, Bernroider and Chudzikowski (2013). Kortjan and Von Solms (2014) have also designed a conceptual framework for cyber-security awareness and education within South Africa that represents a structured approach towards dealing with this ongoing challenge. Al-Hamdani (2014) highlighted the importance of **properly designed** IS security interventions to achieve the objectives of growing IS security maturity. The objective of the research is to contribute towards the appropriateness of interventions (Table 4) and it could, for example, be used in conjunction with Kortjan and Von Solms's conceptual framework.

Although a mere 27% of the respondents showed the appropriate knowledge levels regarding password practices, the results of this study indicated a willingness among ignorant users to improve their password practices. The majority expressed their willingness to obtain more knowledge on password-related matters. The indifference towards IS security may be less than what is commonly believed by IS security professionals as respondents to the survey clearly displayed a readiness to improve their security behaviour. This willingness of users to acquire knowledge suggests an opportunity for those who define IS security intervention learning outcomes to design a process that addresses the drivers of behaviour as identified in this paper.

By improving education and training programs to take cognisance of the determinants of password performance, real sustainable improvement in IS security levels is indeed possible. Besides sharing knowledge on secure password practices, password vulnerability, threats and consequences of violations, these programs should focus on users' ability to apply these practices as well as address the motivational issues. It is only through growing capability and dealing with factors that motivate behaviour that a real difference in IS security maturity can be achieved.

References

Aboelmaged, M.G. 2010. 'Predicting e-procurement adoption in a developing country: an empirical integration of technology acceptance model and theory of planned behaviour', *Industrial Management & Data Systems*, **110**(3): 392-414.

Al-Hamdani, W.A. 2014. 'Design thinking approach in teaching information security', *Information Security Education Journal*, **1**(1): 16-29.

Ajzen, I. 1991. 'The theory of planned behavior', *Organizational behavior and human decision processes*, **50**(2): 179-211.

Ajzen, I. 2014. 'The theory of planned behaviour is alive and well, and not ready to retire: A commentary on Sniehotta, Presseau, and Araújo-Soares', *Health Psychology Review,* Review ahead-of-print: 1-7.

Anderson, C.L. & Agarwal, R. 2010. 'Practising safe computing: A multimethod empirical examination of home computer user security behavioral intentions', *MIS Quarterly*, **34**(3): 613-643.

Anderson, N.H. & Butzin, C.A. 1974. 'Performance = motivation × ability: An integration-theoretical analysis', *Journal of Personality and Social Psychology*, **30**(5): 598.

Bauer, S., Bernroider, E.W., & Chudzikowski, K. 2013. 'End user information security awareness programs for improving information security in banking organizations: Preliminary results from an exploratory study', In *AIS SIGSEC Workshop on Information Security & Privacy (WISP2013),* Milano.

Bélanger, F. & Crossler, R.E. 2011. 'Privacy in the digital age: A review of information privacy research in information systems', *MIS quarterly*, **35**(4): 1017-1042.

Bostrom, R.P. & Heinen, J.S. 1977. 'MIS problems and failures: A socio-technical perspective: The application of socio-technical theory', *MIS quarterly*, **1**(4): 11-28.

Brostoff, S. & Sasse, M.A. 2002. 'Safe and sound: A safety-critical approach to security', *Proceedings of the New Security Paradigm Workshop 2001.* [online] URL: http://hornbeam.cs.ucl.ac.uk/hcs/people/documents/Angela%20Publications/unsorted/p41-brostoff.pdf.

Burcu, B., Cavusoglu, H. & Benbasat, I. 2010. 'Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness', *MIS quarterly,* **34**(3): 523-548.

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.

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.

Charoen, D., Raman, M. & Olfman, L. 2008. 'Improving end user behaviour in password utilization: An action research initiative', *Systemic Practice and Action Research,* **21**(1): 55-72, February.

Clegg, C.W. 2000. 'Sociotechnical principles for system design', *Applied Ergonomics*, **31**(5): 463-477.

Conklin, A., Dietrich, G. & Walz, D. 2004. 'Password-based authentication: A system perspective', *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, 1-10.

Da Veiga, A. & Eloff, J.H. 2010. 'A framework and assessment instrument for information security culture', *Computers & Security*, **29**(2): 196-207.

Davis, M.C., Challenger, R., Jayewardene, D.N. & Clegg, C.W. 2014. 'Advancing socio-technical systems thinking: A call for bravery', *Applied Ergonomics*, **45**(2): 171-180.

Dowding, K. 2010. 'Rational choice theory', *The SAGE Handbook of Governance*, 36.

Drevin, L., Kruger, H.A. & Steyn, T. 2007. 'Value-focused assessment of ICT security awareness in an academic environment', *Computers & Security*, **26**(1): 36-43.

Furnell, S.M. 2007. 'An assessment of website password practices', *Computers and Security*, **26**: 445-451.

Furnell, S.M., Bryant, P. & Phippen, A.D. 2007. 'Assessing the security perceptions of personal internet users', *Computers and Security*, **26**(5): 410-417.

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.

Furnell, S.M., Jusoh, A. & Katsabas, D. 2006. 'The challenges of understanding and using security: A survey of end-users', *Computers and Security*, **25**(1): 27-35.

Gehringer, E.F. 2002. 'Choosing passwords: Security and human factors', *IEEE International Symposium on.Technology and Society,* 369-373.

Hamari, J., Koivisto, J., & Sarsa, H. 2014. 'Does Gamification work? A literature review of empirical studies on Gamification', **In** *System Sciences (HICSS), 2014 47th Hawaii International Conference on* (pp. 3025-3034). IEEE, January.

Hardeman, W., Johnston, M., Johnston, D., Bonetti, D., Wareham, N. & Kinmonth, A.L. 2002. 'Application of the theory of planned behaviour in behaviour change interventions: A systematic review', *Psychology & Health,* **17**(2): 123-158.

Heider, F. 1958. *The psychology of interpersonal relations.* New York: Wiley.

Inglesant, P. & Sasse, M.A. 2010. 'The true cost of unusable password policies: password use in the wild', *Proceedings of CHI 2010 (ACM Conference on Human Factors in Computing Systems)*, April.

ISO/IEC. 2014. ISO/IEC 27000. 'Information technology – security techniques – information security management systems – overview and vocabulary', [online] URL: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

Kortjan, N. & Von Solms, R. 2014. 'A conceptual framework for cyber-security awareness and education in South Africa', *South African Computer Journal*, 52: 29-41, July.

Kritzinger, E. & Von Solms, S.H. 2010. 'Cyber security for home users: A new way of protection through awareness enforcement', *Computers & Security*, **29**(8): 840-847.

Leach, J. 2003. 'Improving user security behaviour', *Computers & Security,* **22**(8): 685-692.

Li, H., Zhang, J. & Sarathy, R. 2010. 'Understanding compliance with internet use policy from the perspective of rational choice theory', *Decision Support Systems*, **48**(4): 635-645.

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.

Mumford, E. 1995. *Effective systems design and requirements analysis: The ETHICS approach*. Macmillan.

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

Paternoster, R. & Pogarsky, G. 2009. 'Rational choice, agency and thoughtfully reflective decision making: The short and long-term consequences of making good choices', *Journal of Quantitative Criminology*, **25**(2): 103-127.

Pfleeger, S.L. & Caputo, D.D. 2012. 'Leveraging behavioral science to mitigate cyber security risk', *Computers & Security*, **31**(4): 597-611.

Sasse, M.A., Brostoff, S. & Wierich, D. 2001. 'Transforming the 'weakest link' – a human/computer interaction approach to useable and effective security', *BT Technology Journal*, **19**(3): 122-131.

Shaughnessy, J., Zechmeister, E. & Jeanne, Z. 2011. *Research methods in psychology*. 9th Edition. New York, NY: McGraw Hill, 161–175.

Sniehotta, F.F., Presseau, J. & Araújo-Soares, V. 2014. 'Time to retire the theory of planned behaviour', *Health Psychology Review,* **8**(1): 1-7.

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

Tam, L., Glassman, M. & Vandenwauver, M. 2010. 'The psychology of password management: A tradeoff between security and convenience', *Behaviour and Information Technology*, **29**(3): 233-244, May-June.

Thornton, D. & Francia III, G.A. 2014. 'Gamification of information systems and security training: issues and case studies', *Information Security Education Journal*, **1**(1): 16-29.

Van Niekerk, J.F. & Von Solms, R. 2010. 'Information security culture: A management perspective', *Computers & Security*, **29**(4): 476-486.

Vance, A. & Siponen, M.T. 2012. 'IS security policy violations: A rational choice perspective', *Journal of Organizational and End User Computing (JOEUC)*, **24**(1): 21-41.

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, January.

Weinstein, N.D. 1980. 'Unrealistic optimism about future life events', *Journal of Personality and Social Psychology*, **39**: 806-820.

Wixom, B.H. & Todd, P.A. 2005. 'Theoretical integration of user satisfaction and technology acceptance', *Information Systems Research*, **16**(2): 85-102.

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

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