This article was downloaded by: [Universitetbiblioteket I Trondheim NTNU]
On: 18 March 2015, At: 03:03
Publisher: Taylor & Francis
Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK

Behaviour & Information Technology
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/tbit20

The psychology of password management: a tradeoff between security and convenience

L. Tam [a], M. Glassman [a] & M. Vandenwauver [b]
[a] Marketing Department, Old Dominion University, Norfolk, VA, USA
[b] Software Sales, IBM, Norfolk, VA, USA
Published online: 31 Jul 2009.

To cite this article: L. Tam, M. Glassman & M. Vandenwauver (2010) The psychology of password management: a tradeoff between security and convenience, Behaviour & Information Technology, 29:3, 233-244, DOI: 10.1080/01449290903121386

To link to this article: http://dx.doi.org/10.1080/01449290903121386

PLEASE SCROLL DOWN FOR ARTICLE

Taylor & Francis makes every effort to ensure the accuracy of all the information (the "Content") contained in the publications on our platform. However, Taylor & Francis, our agents, and our licensors make no representations or warranties whatsoever as to the accuracy, completeness, or suitability for any purpose of the Content. Any opinions and views expressed in this publication are the opinions and views of the authors, and are not the views of or endorsed by Taylor & Francis. The accuracy of the Content should not be relied upon and should be independently verified with primary sources of information. Taylor and Francis shall not be liable for any losses, actions, claims, proceedings, demands, costs, expenses, damages, and other liabilities whatsoever or howsoever caused arising directly or indirectly in connection with, in relation to or arising out of the use of the Content.

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden. Terms & Conditions of access and use can be found at http://www.tandfonline.com/page/terms-and-conditions

Behaviour & Information Technology
Vol. 29, No. 3, May–June 2010, 233–244

Taylor & Francis
Taylor & Francis Group

The psychology of password management: a tradeoff between security and convenience

L. Tam[a]*, M. Glassman[a] and M. Vandenwauver[b]

[a]*Marketing Department, Old Dominion University, Norfolk, VA, USA;* [b]*Software Sales, IBM, Norfolk, VA, USA*

(*Received 15 October 2008; final version received 12 June 2009*)

Despite technological advances, humans remain the weakest link in Internet security. In this study, we examined five password-management behaviours to answer questions about user knowledge of password quality, motivation behind password selection and the effect of account type on password-management behaviour. First, we found that users know what constitutes a good/bad password and know which common password-management practices are (in)appropriate. Second, users are motivated to engage in these bad password-management behaviours because they do not see any immediate negative consequences to themselves (negative externalities) and because of the convenience–security tradeoff. Applying Construal Level Theory, we found that this tradeoff can be positively influenced by imposing a time frame factor, i.e. whether the password change will take place immediately (which results in weaker passwords) or in the future (which results in stronger passwords). Third, we found a time frame effect only for more important (online banking) accounts.

Keywords: password management; password security; Internet security; user management; motivation

Downloaded by [Universitetbiblioteket I Trondheim NTNU] at 03:03 18 March 2015

1. Introduction

Today's Internet affects more and more aspects of our lives at work and home, from information search and communication, to banking and investment. As such, online security has become an important management issue for companies, computer users and society as a whole (Anderson 2006, Anderson and Moore 2006). An online security breach can lead to large losses, both direct (e.g. the fraudulent emptying of a bank account) and indirect (e.g. the time and money involved in securing the site against future breaches and repairing damage to a firm's reputation). Even perceptions of weak online security can have negative consequences, e.g. a negative impact on overall trust of online shopping companies (Yenisey *et al*. 2005).

Due to the serious consequences of security lapses, companies allocate huge budgets to install safeguards to protect access to their systems (Bishop 1991). The increased spending has led to firewalls, authentication systems and other techniques being deployed to keep systems secure. However, despite these ever-increasing expenditures and efforts, there is a variable that no amount of money can control – the user. Focusing on the user is important because, although stronger authentication techniques are available, corporations tend to continue to use a password-based system to control system access. As a result, even the most sophisticated security system becomes useless if users mismanage their passwords (Furnell *et al*. 2006). The focus of this article is to examine the motives behind password-management behaviour, hoping that this knowledge can improve overall password security.

2. Literature review

There is a general understanding of what makes a good password and the importance of good password management (Ashley and Vandenwauver 1999, Schneier 2006) More specifically, Tari *et al*. (2006) describe the Department of Defense's guidelines for passwords, e.g. memorised, used for only 1 year, not written down, randomly assigned. They conclude that these requirements challenge the user's cognitive abilities and ultimately reduce productivity. As such, it is not surprising that this knowledge does not always translate into good password management. This could be because end users either do not know or are overly optimistic about many aspects of the Internet (Campbell *et al*. 2007), especially online security. The prevailing user attitude is, 'Internet security is important, and security breaches can be catastrophic, but it won't happen to me'. This optimism may explain why users, executives (Powell 2006) and even IT professionals mismanage their passwords. For example, in a recent survey of IT professionals, 40% reported writing down their important business network passwords (Millman 2006), which leads to poor

*Corresponding author. Email: Ltam@odu.edu

ISSN 0144-929X print/ISSN 1362-3001 online
© 2010 Taylor & Francis
DOI: 10.1080/01449290903121386
http://www.informaworld.com

Downloaded by [Universitetsbiblioteket I Trondheim NTNU] at 03:03 18 March 2015

security (Tari *et al*. 2006). Although this may not be an issue if the written password is kept in a secured place, it is unlikely that most would take the extra step to do so. Another example of mismanagement is that many users do not change the default passwords of their ATM cards (Naraine 2006). This increases the likelihood that the password might be taken by someone having unauthorised access to the mail. Using the randomly generated, difficult to remember default password also increases the likelihood that the password will be written down. To minimise mismanagement, some have suggested more education or training (Schneier 2007a) to increase users' awareness (Bresz 2004) of the consequences of poor password management (Featherman *et al*. 2006). At the same time, some have suggested that IT departments, not users, should be responsible for Internet security (Evers 2006). This belief ignores the shift in focus from the use of technology (Neumann 1994) to the user as the major method of improving Internet security. In fact, getting users to follow security policies was recently named one of the two biggest people issues for top-level security management (Wilson 2006). The problem is that where the security professional sees prudent, responsible behaviour, users simply see overhead that gets in the way of performing whatever task they are trying to do (Harrison 2006).

Although there has been some research on the human side of user password-management behaviour, it has mostly examined the issue from a 'should' perspective, i.e. users 'should' follow certain policies and 'should' have certain responsibilities (Bresz and Villacres 2004). Human factors issues involved in choosing passwords such as the impact on users of following password requirements, an increase in the number of user accounts, and stricter password requirements have also been discussed (Gehringer 2002) briefly. Other research has focused on people's cognitive ability to remember passwords (Conklin *et al*. 2004) and on the balance between password complexities and people's ability to remember a password (Gehringer 2002).

Schneier (2007b) recently suggested examining the tradeoffs users make with respect to computer security. Applying the negative externality concept from economics to security, he suggests that most users are not concerned about security because they believe the immediate and negative consequences of a security breach will affect others rather than themselves. For example, in the case of web-based email systems, users do not feel the need to use (and remember) a difficult-to-guess password because the web host will be the direct victim of hackers' attacks. People make tradeoffs between security and a number of factors such as money, time, convenience and capabilities. Given the importance of the human element, Schneier calls for using psychological principles to better understand security-related behaviours.

Despite the considerable literature, the existing research does not answer the two questions of most interest to firms: (1) why do users mismanage passwords and (2) what can companies do to encourage users to engage in good password-management behaviour? To answer these questions, we explored the psychological motives behind password-management behaviour. Our application took the form of a web-based survey and an experiment that studied password management issues for two types of accounts: electronic mail (email) and online banking. Study 1, a web-based survey, was an exploratory study designed to learn the motives behind five common password-management behaviours. Study 2, an experiment, was based on the results of Study 1 and examined the security–convenience tradeoff and the time frame effect and how they impact password quality.

The following are some questions posited by our research:

(1) Do users understand what constitutes a secure password and good password-management behaviour or is more education required?
(2) What are the motives behind password selection and password-management behaviours?
(3) Are there any differences in password-management behaviour for different types of accounts?

Our ultimate goal in answering these questions is to determine what firms can do to encourage users to adopt good password-management practices.

3. Study 1: the motives behind common password-management behaviours

The objective of this web-based survey was to help answer our first and second research questions by measuring security knowledge and exploring the motivation behind some common password-management behaviours.

3.1. Participants and procedures

Internet users (university students) were invited to complete a web-based survey about computer passwords. Participants were told that computer password refers to any password needed to access systems through computers, including personal computers, computers at work, email accounts, online chat rooms and online bank accounts. Participants were asked to list their motivation, i.e. the positive and negative

Downloaded by [Universitetbiblioteket I Trondheim NTNU] at 03:03 18 March 2015

thoughts about the following five password-management behaviours:

- choosing a computer password for the first time, e.g. for a new bank account
- changing a password
- letting someone else use their password
- taping their password next to the computer
- sharing a password with family, friends or co-workers.

The first two password-management behaviours (choosing a password for the first time and changing a password) are common yet neutral behaviours. These behaviours are neutral in that they are neither good nor bad, per se. Rather, it is the way the user chooses and changes the password that determines whether the behaviour is good or bad. By understanding how computer users view these behaviours, we can gain insights into how to bring about good password management.

The other three password-management behaviours (letting someone else use your password, taping your password next to the computer and sharing a password with family, friends or co-workers) are behaviours we want users to avoid. They are considered naive mistakes (Stanton *et al*. 2005). We included them to broaden our understanding of the motivation behind password-management behaviour.

After listing their thoughts about the five behaviours, the participants were asked to write one computer password they considered good and one they considered bad and to explain why they chose the particular password. Also, participants gave us personal background and computer use information.

3.2. Results and discussion

A total of 133 participants (48 females, 84 males) from a diverse population (78 White, 38 Black, 10 Hispanic and 7 Asian) completed the survey. The participants had an average of 6.3 years of work experience, and the majority of them (95 (71.4%)) used passwords to access systems at work. Most used online banking services (101 (75.9%)) and all used online communication including email, online messaging and chat rooms in the past 30 days.

3.2.1. Users have password quality knowledge

First, we determined if our participants were able to distinguish between good and bad passwords. This was ascertained by asking, 'Please write down one computer password you consider good'. Next, the respondent was asked, 'Why do you think it is a good computer password?' Identical questions were asked with regard to a bad password. The results showed that most participants (114 (85.7%)) were, in fact, able to evaluate password quality. Using words from the dictionary, simple combinations of digits, or basic personal information such as name, phone number and birthday were mentioned as examples of bad passwords by 127 participants, i.e. 95.4%. They also knew that random combinations of at least eight digits, letters and symbols made good passwords (114 (85.7%)).

After determining that our participants could evaluate password quality, we conducted a content analysis of their positive and negative thoughts about the five behaviours. These thoughts were elicited by asking, 'What positive and negative things come to mind when you think of (behaviour)'. Two authors of this article coded the open-ended responses. Even though the participants listed their positive and negative thoughts about each behaviour separately, the content analysis indicated that the respondents associated similar concepts with all five behaviours, i.e. the motivational aspects were the same; they dealt with some aspect of either convenience or security. The codes and frequency counts of the concepts associated with each behaviour are listed in Table 1.

3.2.2. Convenience versus security

The study revealed that convenience means more than just ease of use for the individual user. It also deals with ease of use for their trusted ones (such as close friends and family members). Although it is a very bad practice, users are willing to share their passwords with these trusted ones (56 (42.1%)). Forgetting passwords and ease of password retrieval are the most frequently mentioned convenience issues (85 (63.9%)). Users want easy-to-remember passwords and, as a result, pick weak passwords and even reuse old passwords to achieve this goal (Gaw and Felten 2006).

Security refers to the protection of information that would invade one's privacy or could be used for a fraudulent purpose such as identity theft. Privacy (i.e. exposing private information to friends, family or co-workers) was the most frequently mentioned security concern (101 (75.9%)). Information being exposed to unknown parties who might use the information improperly but not illegally was second (66 (49.6%)). To our surprise, the least mentioned security concern involved identity theft or being a victim of other illegal activities (29 (21.8%)). This ranking is especially surprising since Bryant and Campbell (2006) found that users understand the risks associated with hackers and viruses.

Downloaded by [Universitetbiblioteket I Trondheim NTNU] at 03:03 18 March 2015

Table 1. Study 1 – positive and negative associations of five common password-management behaviours.

Thoughts and associations	Choosing passwords		Changing passwords		Letting others use passwords		Taping passwords		Giving passwords to family and friends	
	Positive	Negative	Positive	Negative	Positive	Negative	Positive	Negative	Positive	Negative
Convenience	60	83	34	126	45	0	115	0	114	0
'I can make my password easy to remember', 'My trusted ones can remind me of my password upon my request'	35 (58%)		15 (44%)		11 (24%)		115 (100%)		58 (51%)	
'I can use something meaningful to me'	13 (22%)									
'I make passwords all the same/ similar', 'I reuse the old ones'	12 (20%)	11 (13%)	19 (56%)							
'I will/may forget my password'		48 (58%)		85 (67%)						
'I have too many passwords and get confused', 'I will write down my passwords'		24 (29%)		41 (33%)						
'My trusted ones can access my information when needed', 'For the convenience of others'					34 (76%)				56 (49%)	
Security	73	50	99	7	0	133	0	133	0	133
'Good for computer security', 'Information is protected', 'My privacy is protected'	46 (63%)		66 (67%)							
'Others can't access/use my accounts', 'People who knew it don't know anymore'	27 (37%)		33 (33%)	4 (57%)						
'I have to follow their guidelines'		8 (16%)		3 (43%)						
'My personal information is exposed to my friends and family'						63 (47%)		101 (76%)		82 (62%)
'Others can find out my passwords', 'People who I don't trust may have access to my personal information'		31 (62%)				41 (31%)		19 (14%)		42 (32%)
'Fraud', 'Stealing', 'Illegal activities can happen', 'I may get hacked'		11 (22%)				29 (22%)		13 (10%)		9 (6%)
Nothing positive	0		0		88		18		19	
Total	*133*	*133*	*133*	*133*	*133*	*133*	*133*	*133*	*133*	*133*

Table 2. Descriptive of Study 2.

Variables	Mean	Standard deviation
Intention to pick a secure password	5.64	1.27
Intention to pick a convenient password	6.28	0.81
Convenience-security tradeoff	1.62	1.71
Password quality	2.62	1.35

3.2.3. *Bad password management is about convenience*

It has been suggested that users' cognitive ability (i.e. memory) limits their use of strong passwords (Gehringer 2002) and that more user education about the negative consequences of bad password management would encourage good password behaviours (Weiss 2007). However, our research does not support these ideas. It shows that users let someone else use their password, taped a password next to the computer and shared a password with friends, family and co-workers despite knowing these behaviours represented bad password management. They engaged in these activities because they made password management more convenient. Although some have looked to 'pass-phrases' consisting of multiple words familiar to the user to address the convenience (memorability), Keith, Shao, and Steinbart (2007) found that pass-phrases resulted in more failed login attempts than simple or highly secure passwords because of typographical errors.

While forgetting a password was our users' greatest concern, our findings suggest that this concern may, in fact, be overblown. When users were specifically asked how difficult it is to remember their passwords (using a six-point scale with one being extremely difficult, six being extremely easy), the average score was 4.83 (SD = 0.92). Furthermore, no one said it was 'extremely difficult' to remember their passwords. These results suggest that concerns about forgetting one's passwords are not the key factor behind bad password management. The desire for convenience is the motivator behind bad password management. Users are saying, 'If I have to, I can remember my password even if it is complex, but I'd rather not put the mental effort into it. I'd rather write it down and tape it to my computer because it is more convenient ... one less thing to be bothered with'.

In summary, we found that users were more concerned about less harmful privacy issues (e.g. personal information being exposed to friends and family) than about what IT security professionals consider much more harmful (e.g. fraud and identity theft). Our results show that users do understand what a secure password is. However, they associate secure passwords with a loss of convenience (i.e. the security–convenience tradeoff), and they do not want to give up convenience. The results further suggest that more education about the negative consequences of bad password management would not change their behaviour. Do our findings imply that security departments should stop educating users about the importance of good password management and only focus on the technical aspects of protection as suggested by some security experts? (Bresz 2004). The results of our second study, which dealt with choosing passwords and changing passwords, shed insight into this issue.

3.2.4. *Choosing versus changing a password*

In addition to bad password-management behaviour, we also studied two very common, yet important, password-management behaviours: choosing a password for the first time and changing a password. As shown in Table 1, the same convenience and security factors emerged from the analysis of users' positive and negative thoughts regarding each behaviour. Users had both positive and negative associations with each behaviour. When asked to list the positive and negative things that came to mind when choosing a password, both convenience and security were mentioned. As shown in Figure 1, the roles of convenience and security were different for each behaviour. Users realised that increased security was a positive outcome of choosing and changing passwords properly, as there were more thoughts listed about security when asked about positive thoughts than when asked about negative thoughts. We found this pattern for both choosing a password for the first time (55% vs 38%; $t_{(131)} = 2.58$, $p < 0.05$) and changing a password (75% vs 5%; $t_{(131)} = 17.06$, $p < 0.01$). Figure 1 reveals an unexpected yet interesting pattern: users thought of choosing a password for the first time and changing a password differently. Compared with choosing a password for the first time, changing a password elicited more positive thoughts about security (75% vs 55%; $t_{(131)} = 3.75$, $p < 0.01$) and fewer negative thoughts about security (5% vs 62%; $t_{(131)} = 7.83$, $p < 0.01$). In other words, users are mainly concerned about inconvenience when they thought of the negative outcomes associated with changing a password (compared with choosing a password for the first time) and security when they thought of the positive outcomes of changing a password.[1]

This pattern was not expected. However, it provided insights into what causes users to be more concerned about convenience or security. We believe the data suggests that choosing and changing a password carry different implicit time frames. We believe that choosing a password for the first time has a near future and act-now time frame, whereas changing a password has a distant future time frame. We

Downloaded by [Universitetbiblioteket I Trondheim NTNU] at 03:03 18 March 2015

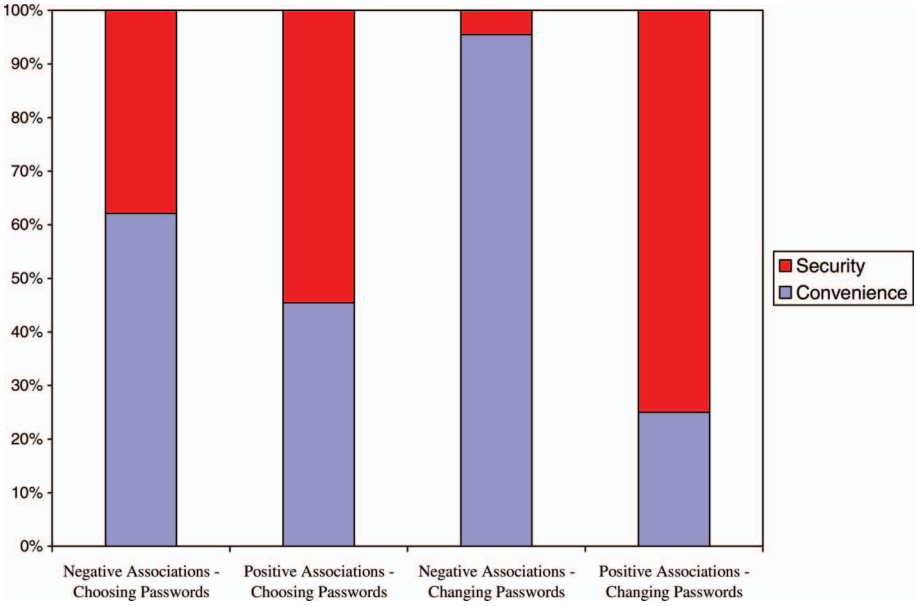

Figure 1. Convenience and security in choosing and changing passwords.

conducted Study 2 to further investigate the time-frame variable.

4. Study 2: convenience versus security and the time-frame effect

On the basis of the findings of Study 1, we concluded that users understand password quality and the negative consequences of risky password-management behaviour. Nevertheless, they are willing to trade security for convenience when choosing a password. This, of course, raises the questions 'What is the underlying motivation for good password management behaviour?', 'What can companies do to encourage users to improve their behaviour?', and 'How does time frame, whether the password expires immediately or in the future, affect password management behaviour?' As mentioned earlier, one of the biggest security problems is the choice of weak passwords (Wilson 2006). The objective of Study 2 is to determine how time frame along with convenience and security affect the most important password-management behaviour, namely selecting a password.

4.1. Time-frame effect

To better understand the time-frame effect found in Study 1, we looked to the psychological literature, specifically to Construal Level Theory (Trope and Liberman 2003). According to this theory, temporal distance changes responses to future events by changing the way people mentally represent those events. The theory states that, for *near future events*, people focus on the more *concrete details* of the events, whereas for *distant future events*, people focus on the more *abstract features*. Therefore, there is a stronger emphasis on desirability (versus feasibility) when thinking about distant future events and a stronger emphasis on feasibility (versus desirability) when thinking about near future events. In other words, there is a tradeoff between feasibility and desirability – people focus on what they desire when thinking about distant future events and what they can realistically do when thinking about near future events. Empirical research (Eyal *et al*. 2004) supports this notion, finding that the 'pros' of the behaviour (desirable outcomes) have a bigger influence on behaviour for events taking place in distant future, whereas the 'cons' of the behaviour (feasibility details) have a bigger influence on behaviour for events taking place in the near future.

In the context of password management, the results of Study 1 suggest that protection from identity theft (security) is a distant future consideration where the focus is on desirability while picking an easy-to-remember password is a near future consideration where the focus is convenience. Combining the notion that security is about desirability and convenience is about feasibility and the tenets of Construal Level Theory, we expect users place a greater emphasis on security (desirability), and thus pick a stronger password, when considering distant future events. We also expect users to place a stronger emphasis on convenience (feasibility), and therefore pick a weaker password, when considering a near future event. We tested this hypothesis with the experimental study described below.

Downloaded by [Universitetbiblioteket I Trondheim NTNU] at 03:03 18 March 2015

Downloaded by [Universitetbiblioteket I Trondheim NTNU] at 03:03 18 March 2015

4.2. Participants and procedures

A total of 140 Internet users not participating in Study 1, recruited and screened the same way, participated. They were provided with the definition of a password used previously. We used a 2 (account types: email account versus online banking account) × 3 (time frame: today versus tomorrow versus 3 weeks later) between-subjects experimental design resulting in six questionnaires, e.g. email-tomorrow. We included three time-frame levels instead of two as suggested by Construal Level Theory because we felt Internet users may have a different sense of time. While we suspected that tomorrow might be regarded as distant future, we wanted to include a time (3 weeks later) that was clearly in the distant future for comparison purposes.

Participants were given one of the six scenarios mentioned earlier and asked: imagine you are logging-in to your email account (or online banking account) and see the following message: 'Your password **has expired** (or will expire tomorrow or 3 weeks from today). Please **choose a new password now** (or be prepared to choose a new password tomorrow or 3 weeks from today)'. Their intentions to pick a convenient and secure password were then measured using seven-point scales (one being strongly disagree and seven being strongly agree). The questions measuring intention to pick a convenient password were: 'I will pick an easy-to-remember password', 'I will pick a password that is convenient to me' and 'I will pick a password that I won't forget'. The intention to pick a secure password was measured by asking: 'I will pick a password that is secure', 'I will pick a password following the suggested guidelines provided by the system' and 'I will pick a password that is hard to guess'. Next, we determined the tradeoff between convenience and security using the following:

> People choose a password for many reasons. Some choose one because it will be easy to remember while others choose one because they feel no one will guess it. Other people choose one that is in between. When you choose the password you will use when you log-on NOW (or tomorrow or 3 weeks from today), how will you choose it? What is important to you? To tell us this, please read the instructions below.
>
> For your new password that you will need NOW (or tomorrow or 3 weeks from today), please allocate 100 points between the ease-of-use of the password and the amount of security the password will provide. For example:
>
> - if you allocate 10 points to security and 90 points to ease-of-use, the password will be very easy to remember, but not very secure, i.e. it will be easy to 'crack (guess)'.
> - if you allocate 85 points to security and 15 points to ease-of-use, it will be very difficult to 'crack (guess)', but not necessarily easy to remember.
> - if you allocate 50 points to each, the password will provide some level of security and be somewhat easy to remember.

Finally, users gave us an example of the password they would choose in the scenario provided.

4.3. Results and discussion

The scores of the intentions to choose convenient (reliability $\alpha = 0.75$) and secure passwords (reliability $\alpha = 0.76$) were averaged to form the two intention measurements. A security–convenience tradeoff score was constructed by dividing the points allocated to security by the points allocated to convenience in the tradeoff question. The quality (level of security) of the password provided by the user was coded into one of the five following categories:

(1) words, names or numbers (six digits or less) – low security
(2) words or names that include capital letters
(3) a combination of words and digits
(4) a random combination of letters
(5) a random combination of special characters, letters and digits – high security.

The dependent variables analysed were the intention to pick a convenient password, the intention to pick a secure password, the security–convenience tradeoff score and the password quality. No gender differences were found in any of the dependent variables ($ts_{(138)} < 0.46, ps > 0.64$). Another, somewhat surprising, finding was that there were no noticeable differences in any of the dependent variables (intention to pick a convenient password, intention to pick a secure password, security–convenience tradeoff score and password quality) between users who used passwords at work and users who did not ($ts_{(138)} < 0.42, ps > 0.68$).

4.3.1. Negative externality affects password-management behaviour

As displayed in Figure 2, our findings confirm the negative externality concept (Anderson and Moore 2006) that states that people are not concerned about the negative consequences of their behaviour if they believe the immediate and negative consequences only affect others. In other words, users are not concerned about security issues unless they feel they will be affected if the account is misused. We found that

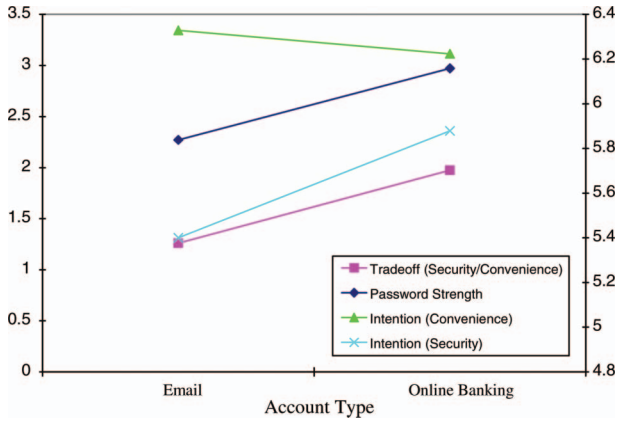

Figure 2. Negative externality in email versus online banking accounts.

password quality was significantly higher for online banking (where users see an immediate and negative impact as a result of having their accounts compromised) than for email accounts (2.97 vs 2.27, $t_{(138)} > 3.16$, $p < 0.01$). Also, users' overall intention to pick a secure password was higher for online banking than for email accounts (5.89 vs 5.40, $t_{(138)} > 2.27$, $p < 0.05$). Convenience is a 'must-have' factor. Users' intention to pick a convenient password was high with no significant difference between online banking and email accounts (6.22 vs 6.32, $t_{(138)} < 0.76$, $p > 0.44$). It seems as though users were willing to sacrifice convenience for security only when the immediate consequences of having their password misused were more negative, such as experiencing a personal financial loss. The negative externality proposition was further supported by the significant difference in security–convenience tradeoff scores between email and online banking accounts (1.26 vs 1.98, $t_{(138)} > 2.51$, $p < 0.05$).

4.3.2. *Determinants of password quality*

Next, we used regression analysis to determine which factor is more important in determining the quality of the chosen password, the intention to pick a secure password or the tradeoff between convenience and security (Note: the intention to pick a convenient password was not included in subsequent analysis as there was no difference between email and banking accounts). Consistent with results of Study 1, convenience was regarded as a hygiene factor in that all users wanted an easy-to-remember password.

We compared the impact of the intention to pick a secure password and the impact of the convenience–security tradeoff using regression analysis. Using the tradeoff score and the intention to pick a secure password as independent variables and password quality as the dependent variable, we found the convenience–security tradeoff was significant ($t_{(138)} = 2.58$, $p < 0.05$) while the intention to pick a secure password was not significant ($t_{(138)} = .78$, $p > 0.43$) in determining the actual quality of the password chosen by the user.[2]

This leads us to a very important conclusion. Contrary to common belief, having an intention to pick a secure password does not result in picking a better password. However, the willingness to trade convenience for security does explain why users pick a stronger password. This means people choose a secure password not because they know it is secure, but because they are willing to sacrifice convenience. Only if people are willing to sacrifice convenience, will they choose stronger passwords.

4.3.3. *Time-frame effect*

Given the importance of the security–convenience tradeoff in determining password quality, the next important question becomes, what affects user's willingness to trade convenience for security? As discussed earlier, the type of account is one possible explanation for users being more willing to give up convenience for security. Is externality the only explanation for this finding? If account type is the only variable that affects password-management behaviour including the quality of password chosen, then why do some users fail to change the default passwords of their ATM cards (Millman 2006) or reuse their old passwords? From Study 1, it was determined that the implicit time frame might have a significant influence on password quality as well. In Study 2, the time-frame effect is explicitly tested. As shown in Figure 3, we propose that different account types and the time frame interact to affect the tradeoff between convenience and security, affecting password quality.

To test the proposed framework, the three-step procedure outlined by Baron and Kenny (1986) was followed. First, a 2 (account types: online banking versus emails) × 3 (time frame: now versus tomorrow versus 3 weeks later) ANOVA (analysis of variance) with security–convenience tradeoff as dependent variable was conducted. That is, we used ANOVA to compare the average convenience–security tradeoff scores for online banking versus email accounts and for password expiration time frames of now versus tomorrow versus 3 weeks later. We also looked to see whether account type and time frame interacted to affect tradeoff scores. The ANOVA revealed a significant two-way interaction between account type and time frame ($F_{(1,\ 134)} = 4.09$, $p < 0.05$) and no significant main effect of account type ($F_{(1,\ 134)} = 3.79$, $p > 0.05$) or of time frame ($F_{(1,\ 134)} = 0.41$, $p >$

Downloaded by [Universitetsbiblioteket I Trondheim NTNU] at 03:03 18 March 2015

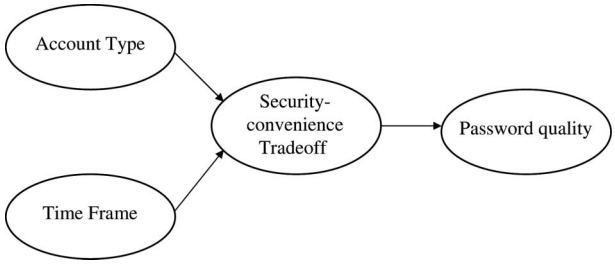

Figure 3. Tradeoff perspective of password-management behaviour.

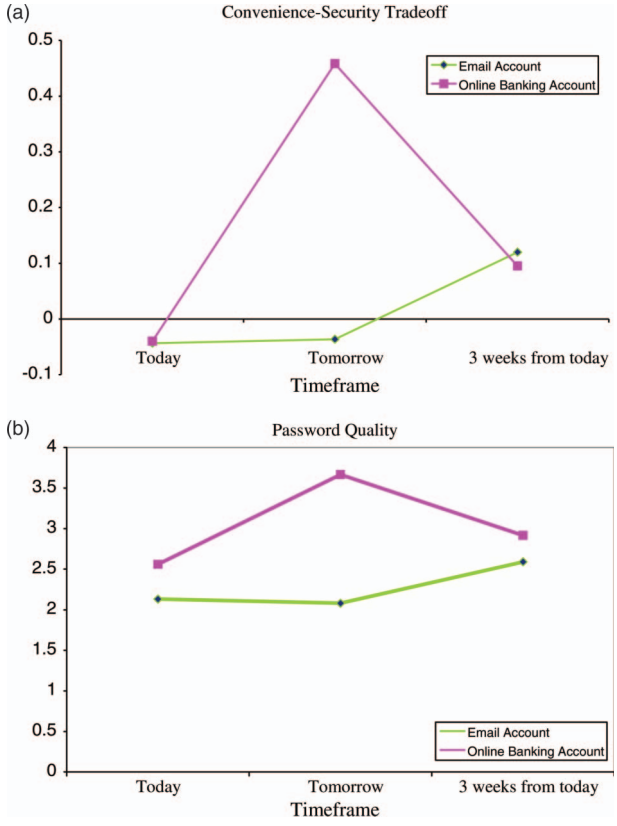

Figure 4. (a) Time frame, account type, and tradeoff effects on convenience–security tradeoff. (b) Time frame, account type, and tradeoff effects on password quality.

0.66). Next, another ANOVA with the same independent variables (account type and time frame) but a different dependent variable (password quality) was conducted. This revealed a significant two-way interaction between account type and time frame ($F(1, 134) = 3.11$, $p < 0.05$) and a significant main effect of account type ($F(1, 134) = 11.74$, $p < 0.01$) but no significant time frame main effect ($F(1, 134) = 2.01$, $p > 0.14$). Finally, the same 2 (account types) × 3 (time frame) ANOVA with password quality as dependent variable and convenience–security tradeoff as a covariate was conducted. The mediator role of the convenience–security tradeoff in determining password quality is supported as this analysis showed a significant convenience–security tradeoff effect ($F(2, 132) = 6.30$, $p < 0.01$) and a non-significant two-way interaction of account type and time frame ($F(2, 132) = 2.61$, $p > 0.07$).

As the framework in Figure 3 is supported, we want to know how account type and time frame together affect the convenience–security tradeoff and password quality. From Figures 4a and b, we can conclude that time frame does not have the same effect on the two account types with respect to the convenience–security tradeoff. For more important (online banking) accounts, the planned contrast shows that giving users just enough time to choose or change a password (time frame: tomorrow) results in a tradeoff preference for security (0.46 vs 0.02, $F(1, 134) = 4.61$, $p < 0.05$) and higher password quality (3.43 vs 2.78, $F(1, 134) = 5.76$, $p < 0.05$). In other words, giving users too little (time frame: today) or too much (time frame: 3 weeks from today) time to choose their passwords results in a tradeoff preference for more convenience (and thus less security) resulting in weaker passwords. The results seem to be inconsistent with Construal Level Theory, which suggests that users should be more willing to trade convenience for security for events expected to happen in distant future (that is, the 3 weeks from today). However, as explained earlier, users probably interpret online and offline time frames differently. The '3 weeks from today' time frame may not evoke any immediate responses since users may not consider changing their passwords until they are about to expire.

On the other hand, the findings were different for less important (email) accounts. The time-frame effect found for the more important (online banking) account disappears for both the convenience–security tradeoff ($F(2, 134) = 2.12$, $p > 0.12$) and password quality ($F(2, 134) = 0.20$, $p > 0.81$). Users are not willing to give up convenience for better security for these types of accounts, and therefore, they do not choose strong passwords.

5. Conclusions and discussion

We posited three questions at the beginning of the article. First, do users understand what constitutes a secure password or is more education required? Second, what are the motives behind password selection and password-management behaviours? Third, are there any differences in password-management behaviour for different types of accounts? With respect to the first question, the results support the idea

Downloaded by [Universitetbiblioteket I Trondheim NTNU] at 03:03 18 March 2015

Downloaded by [Universitetbiblioteket I Trondheim NTNU] at 03:03 18 March 2015

that users understand the difference between good and bad passwords and the consequences of bad password-management behaviour.

With respect to the second question, we found that the motives behind password selection and password-management behaviours are complex. First, the concept of security has different meanings to different users. In our study, 86% of users are more motivated by personal privacy issues than security issues. Second, the fear of forgetting a password motivates users to choose simple passwords and engage in bad password-management behaviours. However, the fear of forgetting a password may be overblown. Our study shows that users do not have difficulty remembering passwords. Third, the time frame of password selection affects the motivation to choose a secure password. The motives behind changing a password versus choosing one for the first time are different. As with security professionals, users are motivated by security and by convenience and make tradeoffs between them when choosing passwords. It is the convenience–security tradeoff that determines password quality, not the intention to choose a secure password. Therefore, users choose strong passwords only if they are willing to sacrifice convenience; it is not sufficient for them to understand it is important to choose a strong password. In our study, we found that 36.4% (51 participants) were willing to sacrifice security for convenience.

We found differences in password-management behaviour for different types of accounts, thereby answering our third question. Consistent with the negative externality concept, users pick stronger passwords and are more willing to sacrifice convenience for security for those accounts for which there is an immediate negative consequence when the account is compromised. For bank accounts, there is a significant time-frame effect – users pick a stronger password when they have 1 day to memorise it and a weaker password when they have too little or too much time to learn the password. The time-frame effect disappears for email accounts – users are simply not willing to give up any convenience when choosing passwords for such accounts.

In view of our findings, some of which contradict contemporary thought about user education, we have a few suggestions for companies using password-based security systems. First, do more than just make users aware of the importance of the account for which they have to manage a password by making them also understand the negative consequences of poor password management. Users must feel a *personal loss* if the account is compromised. Second, implement an enterprise single sign-on solution. This eliminates the need for users to remember multiple passwords. Users are more likely to trade convenience for security if they have to remember only one password. Third, if single sign-on is not available, allow users to write down their passwords if they put the notes in a safe place. Fourth, if password aging is used to force users to change their passwords frequently, send them a warning message that they have to change their password 1 day before the change is actually enforced. Do not send the message weeks beforehand, and do not wait until the day the change is required. Lastly, keep users informed about security issues such as hacker attempts on the system. However, do not overspend by trying to teach them what constitutes a good password because most of them already know this. In our study, 85.7% knew what constituted a good password. For those who do not know what constitutes a good password, online training and password quality checking is available.

This research provides a new way of looking at password-management behaviour. Using Construal Level Theory, we found that the security–convenience tradeoff plays a major role in determining password quality. In contrast to the traditional belief that an understanding of the importance of online security leads to better password-management behaviour, our studies show that only users who are willing to trade convenience for security choose strong passwords. Moreover, we found that the security–convenience tradeoff effect is stronger for more important accounts (online banking accounts) than for less important accounts (email accounts). In addition, the time frame influences the security–convenience tradeoff effect. An immediate time frame leads to weaker passwords than a more distant time frame.

Despite the insights provided by our studies, other questions must be answered if password-management behaviours are to be improved. First, what other factors affect the convenience–security tradeoff? Second, selecting a strong password is only one of many good password-management behaviour users perform. Can our framework be applied to other password-management behaviours such as changing passwords, frequently? Finally, the habit literature (e.g. Wood *et al.* 2005) suggests that people with strong habits are not rational if the circumstances remain the same. Therefore, bad habits remain unless circumstances change. Bad password-management habits such as taping passwords next to the computer, not changing default passwords and reusing old passwords only change if circumstances change. Hence, strict controls with significant consequences when finding password rule violations are a must. Although there is a clear need for future research, we believe the research presented here provides the first step towards improved password-management behaviour by understanding the psychological aspects of password management.

Downloaded by [Universitetbiblioteket I Trondheim NTNU] at 03:03 18 March 2015

Notes

1. Before presenting the results of Study 2, we would like to address a possible alternative explanation for our findings: risk taking. It is possible that risk takers were consistently less concerned about security (and more about convenience) while those who were risk avoidant were more concerned about security (and less about convenience). To address this issue, we measured both general and password management risk propensity. Risk taking as a general personality trait and risk taking as it relates to password management were both measured on a seven-point scale (one being strongly disagree and seven being strongly agree). The reliabilities of the two scales were $\alpha = 0.81$ and $\alpha = 0.74$ for general personality trait and password management, respectively. Next, the scores of the two scales were averaged. There were no differences in risk-taking propensities (as a general personality and to password management) between users who were more concerned about convenience and those who were more concerned about security with respect to the positive and negative thoughts that were elicited when asked about choosing a first-time password or changing a password ($ts_{(130)} < 1.2$, $ps > 0.22$).
2. An alternative explanation for our findings is that the security–convenience tradeoff variable was strongly correlated with the intention to pick a secure password. A high correlation between these two variables would result in the security–convenience tradeoff variable having a greater impact in determining actual password quality than the intention to pick a secure password. To rule out this possible explanation, we examined the bivariate correlations among password quality, the security–convenience tradeoff and the intention to pick a secure password. There was a significant relationship between the security–convenience tradeoff and password quality (correlation $\gamma = 0.24$, $p < 0.01$) but not between the intention to pick a secure password and password quality (correlation $\gamma = 0.12$, $p > 0.13$). This means the relationship between the intention to pick a secure password and password quality is much weaker than between the security–convenience tradeoff variable and password quality.

References

Anderson, K.B., 2006. Who are the victims of identity theft? The effect of demographics. *Journal of Public Policy and Marketing*, 25 (2), 160–171.

Anderson, R. and Moore, T., 2006. The economics of information security. *Science*, 314, 610–613.

Ashley, P. and Vandenwauver, M., 1999. *Practical Intranet Security: Overview of the State of the Art and Available Technologies*. Boston, MA: Kluwer Academic.

Baron, R. and Kenny, D., 1986. The moderator-mediator variable distinction in social psychological research: conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, 51 (6), 1173–1182.

Bishop, M., 1991. Password management. *COMPCON 1991 Proceedings*, 167–169.

Bresz, F.P., 2004. People – often the weakest link in security, but one of the best places to start: without awareness and training, security compliance is not possible. *Journal of Health Care Compliance*, 6 (4), 57–61.

Bresz, F.P. and Villacres, C., 2004. Controlling authentication in a health care environment: multi-factor mechanisms may be one option for your organization. *Journal of Health Care Compliance*, 6 (6), 52–54.

Bryant, K. and Campbell, J., 2006. User behaviours associated with password security and management. *Australasian Journal of Information System*, 14 (1), 81–100.

Campbell, J., *et al*., 2007. Unrealistic optimism in internet events. *Computers in Human Behaviour*, 23, 1273–1284.

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

Evers, J., 2006. Security expert: user education is pointless. *CNet News* [Online]. Available from: http://news.com.com/2102-7350_3-6125213.html

Eyal, T., *et al*., 2004. The pros and cons of temporally near and distant action. *Journal of Personality and Social Psychology*, 86 (6), 781–795.

Featherman, M.S., Valacich, J.S., and Wells, J.D., 2006. Is that authentic or artificial? Understanding consumer perceptions of risk in e-service encounters. *Information Systems Journal*, 16, 107–134.

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

Gaw, S. and Felten, E.W., 2006. Password management strategies for online accounts. *In*: *Symposium on Usable Privacy and Security (SOUPS)*, July 12–14, Pittsburgh, PA, USA.

Gehringer, E., 2002. *Choosing passwords: security and human factors*. *2002 International Symposium on Technology and Society*, 369–373.

Harrison, W., 2006. From the editor: passwords and passion. *IEEE Software*, July/Aug. 5–7.

Keith, M., Shao, B., and Steinbart, P.J., 2007. The usability of passphrases for authentication: an empirical field study. *International Journal of Human-Computer Studies*, 65 (1), 17–28.

Millman, R., 2006. Four in ten security staffers write down passwords. *SC Magazine*, June 13.

Naraine, R., 2006. Googling for ATM masters passwords. *eWeek.com*, 21 Sept.

Neumann, P., 1994. Risks of passwords. *Communications of the ACM*, 37 (4), 126.

Powell, J., 2006. How security breaches impact your brand. *Enterprise Systems*, 31 Oct.

Schneier, B., 2006. *Beyond fear: thinking sensibly about security in an uncertain world*. New York: Springer Science+Business Media, LLC.

Schneier, B., 2007a. *Secure passwords keep you safer* [Online]. Available from: www.wired.com/news/columns/1,72458-0.html

Schneier, B., 2007b. The psychology of security [Online]. Available from: http://www.schneier.com/essay-155.html [Accessed 18 January 2008].

Stanton, J., *et al*., 2005. Analysis of end user security behaviors. *Computers & Security*, 24, 124–133.

Tari, F., Ozok, A., and Holden, S., 2006. A comparison of perceived and real shoulder-surfing risks between alpha-numeric and graphical passwords. *In*: *Proceedings of SOUPS 2006 Symposium on Usable Privacy and Security*, 56–66.

Trope, Y. and Liberman, N., 2003. Temporal construal. *Psychological Review*, 110 (3), 403–421.

Weiss, T., 2007. Study: weak passwords really do help hackers. *Computerworld*, 7 February.

Wilson, T., 2006. It's the people, stupid [Online]. Available from: http://www.darkreading.com/document.asp?doc_id=108163 [Accessed 24 October 2006].

Wood, W., Tam, L., and Witt, M., 2005. Changing circumstances, disrupting habits. *Journal of Personality and Social Psychology*, 88 (6), 918–933.

Yenisey, M., Ozok, A., and Salvendy, G., 2005. Perceived security determinants in e-commerce among Turkish university students. *Behaviour & Information Technology*, 24 (4), 259–274.

Downloaded by [Universitetbiblioteket I Trondheim NTNU] at 03:03 18 March 2015