South African Journal
of Information Management
[ DoE accredited ]

Peer Reviewed Article Vol.9(2) June 2007

# Assessment of current practices in creating and using passwords as a control mechanism for information access

**P.L. Wessels**
Department of Accounting, Stellenbosch University
Stellenbosch
South Africa
plw@sun.ac.za

**L.P. Steenkamp**
Department of Accounting, Stellenbosch University
Stellenbosch
South Africa
lsteenkamp@sun.ac.za

One of the critical issues in managing information within an organization is to ensure that proper controls exist and are applied in allowing people access to information. Passwords are used extensively as the main control mechanism to identify users wanting access to systems, applications, data files, network servers or personal information. In this article, the issues involved in selecting and using passwords are discussed and the current practices employed by users in creating and storing passwords to gain access to sensitive information are assessed. The results of this survey conclude that information managers cannot rely only on users to employ proper password control in order to protect sensitive information.

**Key words**: Passwords, password control, control of sensitive information, creating and using passwords

Received 5 February 2007; accepted 20 May 2007

**Contents**

---

## 1 Introduction and problem statement

### 1.1 Introduction

Most managers would agree that good information is essential to the success of an organization. Good information, it is believed, improves decision making, enhances efficiency and provides a competitive edge to the organization that knows more than its opposition (Kaye 1995:5). However, this information should be protected from unauthorized access to ensure that the organization retains its competitive edge. One of the critical issues in managing information within an organization is to ensure that proper controls exist and are applied in allowing people access to information. With most organizations using computerized information networks to distribute information to its employees, the development and application of proper controls are critical in denying unauthorized users access to sensitive information. If each employee is supplied with a login name and password, users can be identified by the information system to allow them access to specific information.

With the growth in the use of Web-centred information systems, users can also gain access to outside networks or to specific personal information (e.g. banking details) by supplying a valid login name together with a password selected by them. By using passwords, these users can prove who they are and unauthorized access can be blocked. Passwords have therefore become users' identity cards for accessing internal networks as well as personal accounts on the Internet. However, by the same token, should a malicious user steal or discover an individual's password, he or she can take on the identity of that user.

Passwords are used extensively as the main control mechanism to identify users in order to allow them access to systems, applications, data files, network servers or personal information. The protocol used to verify a password is quite simple. It usually involves comparing an encrypted version of the password with a stored encrypted copy. The weakness is the difficulty users have in remembering all their passwords and personal identification numbers (PINs) without writing them all down (i.e. in an unencrypted format) and posting them in an obvious place, or using easily guessed personal information as passwords. Although one can invent an infinite number of passwords, the security of passwords is still often illusory, given the many social means available to obtain a password through personal knowledge or eavesdropping, and the powerful tools now available for guessing them (Weinshall and Kirkpatrick 2004).

Although creating a good password is not difficult, with so many services requiring password authentication, remembering them can be a problem, especially as the objective is to avoid having a series of numbers and letters that are easy to guess or remember. To prevent users from having to remember a variety of different complex passwords, many use the same password for different applications and services. Unfortunately, this increases the risk of an attacker stealing users' digital identities, as the password could be stored in applications and potentially be accessible to others. Password authentication therefore

appears to involve a trade-off. Some passwords are very easy to remember, but also very easy to guess with dictionary searches or by obtaining the personal information of a user. In contrast, some passwords are very secure against guessing, but difficult to remember (Yan, Blackwell, Anderson and Grant 2004:26–27).

In this article, the issues involved in selecting and using passwords are discussed and the current practices employed by users in creating and storing passwords to gain access to sensitive information are assessed. The literature review undertaken to identify current and past research on password selection and memorability is discussed in the first part. In the second part, the empirical results of a survey that was conducted among undergraduate students who studied Information Systems at a South African university as part of their degree programme are discussed to assess the practices employed by these students to create and use passwords.

### 1.2 Problem statement

The wide publicity received by the increasing number of cases of identity theft (e.g. through phishing), has resulted in a lot more emphasis being placed on advising users on the selection and use of passwords (e.g. Butler 2005). The question now arises as to whether users have changed their practices in selecting and using passwords. The purpose of this research was to assess what practices users currently employ to create and use passwords for accessing their on-line accounts.

### 1.3 Research method

A literature study was undertaken with the specific aim of identifying good practices relating to passwords and of identifying specific issues from past research in this field of study. The literature study did not focus on passwords specifically used on the Internet, but rather on passwords in general, as the principles are generic to different environments. In addition, the literature study identified the background to the use of passwords and the benefits associated with using passwords. A questionnaire was developed on the basis of the good password practices identified from the literature study to assess the current practices employed by users when they select and use passwords to access information.

#### 1.3.1 Questionnaire design

The questionnaire focused on identifying the password practices employed in accessing Internet accounts or information that requires users to identify themselves by providing valid passwords. When the questionnaire was designed, a number of questions were compiled to identify how users currently use passwords (e.g. the number of accounts they use that require passwords, the type of accounts or information that they access with their passwords, whether they use the same password for more than one account and whether they change their passwords on a regular basis). A number of questions were also designed to identify how users currently choose or select their passwords. Their knowledge of good practices regarding password selection [e.g. the length of passwords, the password itself (lower case, personal information, etc.)] and the way that they remember their password was taken into account. The questionnaire was distributed to two lecturers in the auditing field as well as to ten volunteers from the general student population. They were requested to consider the questionnaire in terms of logic and intelligibility. Minor adjustments were made on the basis of their feedback.

#### 1.3.2 Survey

The questionnaire was prepared and distributed with the aid of WebCT. WebCT is a teaching tool that is used at Stellenbosch University and that allows surveys to be conducted electronically. The questionnaire was distributed to all the students enrolled for Information

Systems at first, second and third-year level in the Faculty for Economic and Management Sciences at Stellenbosch University (total population of 1603). In selecting students from various years of study, the researches were able to identify whether users apply better password practices as they become more technology literate and aware of the dangers of identity theft. Although the population existed only of students from one university studying a specific degree programme, the authors felt that these students (studying a commerce degree programme) had sufficient knowledge of information technology and the use of passwords to determine how typical Internet users use and remember their passwords.

The students were all supplied with a login name and password to access the internal network of the University to engage in financial and other transactions (e.g. accessing personal information) that required them to employ good password practices. One expected these students (because of their studies) to be more aware of issues relating to the misuse of passwords and identify theft resulting in the more appropriate management of their password usage than the average student and thus more in line with the typical Internet users employed by business.

The students were requested by e-mail to complete the questionnaire in their own time on a voluntary basis within a time frame of one month ending on 30 November 2006.

The answers to the survey were exported to a spreadsheet application where the data were first cleaned and then analysed. All answers were scrutinized to eliminate instances where students clearly had not answered the questions.

top

## 2 Literature review

Although a vast number of research studies have been done on what good password practices entails, a limited number of studies on how users employ and remember passwords could be identified. Password systems are used extensively to protect users from others gaining unauthorized access to their personal information and systems. It is much safer to use a password on the Internet than securing computers and internal systems. When every possible key is being tested on a personal computer with the actual cipher text, it is a much quicker process than when the testing is being done remotely. Most Web sites will also shut down an account if there are too many incorrect password attempts in a row. That is why criminals have turned to stealing passwords, for example, through phishing (Schneier 2004).

Password-protected accounts are very common and are widely used for a variety of on-line applications, including instant messaging, personal and business e-mail, and on-line banking and retail accounts. Good passwords generally involve a combination of uppercase and lowercase letters at least six to eight characters long, with numbers or special keyboard characters imbedded in the middle (Andrews 2002:16; Armstrong 2002:89; Harada and Kuroki 1996:21–33). Aside from poor password construction, bad practices in password applications include things such as using the same password repeatedly (Dhamija and Perrig 2000), writing down passwords (Barton and Barton 1984:190) and posting passwords in obvious locations such as on a computer monitor (Adams and Sasse 1999:45–46).

Riley (2006) conducted a study among undergraduate and graduate-level college students from Wichita State University in Kansas, USA, to assess what practices users employ to create and store passwords for on-line accounts. The majority of the participants reported password-generation practices that are simplistic and a security risk. Particular practices reported included using lowercase letters, numbers or digits, personally meaningful words and numbers. These findings are supported by similar research by Bishop and Klein (1995)

and Vu, Bhargav and Proctor (2003:1331–1332), who found that even with the application of password guidelines, users tended to revert to the simplest possible strategies (Proctor, Lien, Vu, Schultz and Salvendy 2002:167–168). In her findings, Riley (2006) reported that nearly 60% of the respondents did not vary the complexity of their passwords to match the nature of the site, and 53% indicated that they never change their password if they were not required to do so. These practices were most likely encouraged by the fact that users maintained multiple accounts (average 8,5) and had difficulty recalling too many unique passwords.

It would seem a logical assumption that the practices and behaviours users engage in would be related to what they think they should do in order to create secure passwords. This does not seem to be the case, as participants in Riley's study (2006) were able to identify many of the recommended practices, despite the fact that they did not use the practices themselves. These findings contradict the ideas put forth by Adams and Sasse (1999) and Gheringer (2002), who state that users are largely unaware of the methods and practices that are effective for creating strong passwords. Davis and Ganesan (1993:14–15) point out that the majority of users are not aware of the vulnerability of password-protected systems, the prevalence of password cracking, the ease with which it can be accomplished, or the damage that can be caused by it. While the majority of password users demonstrate technical knowledge of password practices, further education regarding the vulnerability of password-protected systems would help users form a more accurate mental model of computer security.

Yan *et al.* (2004) highlight the problem of selecting good passwords caused by a lack of proper advice to users on how to decide on a password, as well as the system-level enforcement that should complement the password-selection process. Their research consisted of an experiment involving 400 first-year students at Cambridge University. The experiment compared the effects of giving three alternative forms of advice about password selection, and measuring the effect that this advice had on the security and memorability of passwords. In their research they confirmed that users had difficulty remembering random passwords. Passwords based on mnemonic phrases are harder for an attacker to guess than naively selected passwords. A mnemonic phrase involves choosing a password by using the first letters of a phrase or sentence.

However, they found that random passwords were not better than those based on mnemonic phrases, nor were passwords based on mnemonic phrases harder to remember than naively selected passwords. They advise that users should be instructed to choose mnemonic-based passwords, as these are just as memorable as naively selected passwords, while being just as hard to guess as randomly chosen ones. Length of passwords does matter and users should be forced to select passwords of eight characters or more. They also recommend that users should be told to choose passwords that contain numbers and special characters as well as letters.

Compliance with these rules is a critical issue. In systems where users can place only themselves at risk, it may be prudent to leave them to select and change their passwords themselves. In systems where a user's negligence can impact on other users too, consideration should be given to enforcing password quality through system mechanisms. Many of the shortcomings of password-authentication systems arise from human memory limitations. Human memory for sequences is temporally limited, with a short-term capacity of around seven, plus or minus two items. In addition, when humans do remember a sequence of items, those items must be familiar chunks such as words or familiar symbols. Finally, human memory thrives on redundancy and is much better at remembering information encoded in multiple ways (Yan *et al.* 2004:25).

Adams and Sasse (1999:45) note that users are not enemies of security, but collaborators who need appropriate information to help maintain system security. They observe that, when

not told how to choose good passwords, users make up rules for password generation, which results in insecure passwords. The authors conclude that when users create or change their passwords, they should have information available on the best way(s) to construct and memorize a strong password.

In a survey conducted by Brown, Bracken, Zoccoli and Douglas (2004:644) to evaluate the generation and use of passwords, it was found that students in their study had an average of 8,18 password uses. These included the use of passwords to access Internet accounts, as well as for ATM access, cell phone access, etc. The most common items requiring passwords were (in order of frequency) e-mail, voice mail, ATM, access to mainframe and the Internet. With 4,45 different passwords to cover these functions, the average password had 1,84 applications. Two thirds of the passwords were designed around the respondents' personal characteristics, with most of the remainder relating to relatives, friends or lovers. Proper names and birthdays were the primary information used in constructing passwords, accounting for about half of all password constructions. Almost all respondents reused passwords, and about two thirds of password uses were duplications.

The research, as discussed in this section, highlights the issues around the use of passwords in accessing protected information. Given the sensitivity of the information that the users gain access to by supplying a valid password (such as company information, personal information, banking details, etc.), one might expect users to consciously create very secure passwords. As was discussed in this section, this has not proven to be the case, with many studies concluding that users consistently use very simplistic, easily predictable practices when constructing and using passwords. Such predictable and systematic practices are easier for the user to remember, but they sacrifice the security that passwords are intended to provide.

Password authentication therefore involves a trade-off. Some passwords are easy to remember, but also easy to guess. Other passwords are secure against guessing but difficult to remember. This limitation can compromise the password's security, because the user might keep an insecure written record of it or resort to insecure backup authentication procedures after forgetting it.

top

## 3 Results

In the current study, the questionnaire was sent to 1603 students enrolled in Information Systems at either first, second or third-year level, and 519 usable replies were received. These replies were distributed between the various years of study as depicted in Table 1.

**Table 1** Stratified population

| Year of study | Number of replies | Population | Response rate |
|---|---|---|---|
| 1st year | 203 | 780 | 26% |
| 2nd year | 153 | 433 | 35% |
| 3rd year | 163 | 390 | 42% |
| **Total** | **519** | **1603** | **32,4%** |

The response rate of 32,4% was considered sufficient to draw meaningful conclusions. No differentiation is made between the different groups in discussing the findings, as the results were consistent between the groups.

### 3.1 Current uses of passwords

A number of questions dealt with the current practices employed by users in accessing Internet accounts that require passwords.

The average number of Internet accounts requiring respondents to use passwords was 3,22, with a standard deviation of 2,17. Of the 519 respondents, 102 indicated that they had three accounts requiring passwords. The highest sensible response was one respondent with twelve accounts requiring passwords. The average number of passwords used was 1,88, with a standard deviation of 1,15. From this it was evident that respondents regularly used the same password on more than one account, with each password having on average of 1.7 uses. The finding of this survey of 3,22 different password accounts and 1,88 unique passwords is in line with the findings as reported by Brown *et al.* (2004:644), namely 8,18 password uses with 4,45 unique passwords.

The respondents were asked to indicate the Internet account that they used most frequently. In Table 2 the results of their responses are depicted.

**Table 2** Type of account

| | | |
|---|---|---|
| Other | 174 | 34% |
| Internet-based e-mail (excluding the university's e-mail) | 129 | 25% |
| Web site for information (e.g. PCMag.com) | 78 | 15% |
| Internet banking | 59 | 11% |
| On-line chat site | 32 | 6% |
| Subscription to mailing list | 20 | 4% |
| Not answered | 19 | 4% |
| On-line shop (e.g. Kalahari.net) | 8 | 1% |
| **Total** | **519** | **100%** |

The highest usage of an Internet account as indicated in the survey was for Internet-based e-mail, with 25% of the students indicating that this was the Internet account they accessed the most. Eleven per cent of students indicated that the Internet account they used most frequently was for Internet banking. This is of particular relevance, as the security surrounding Internet banking (and therefore the use of secure passwords) should be high.

The poor practice most frequently cited in the literature is using the same password for more than one secure Internet account. Respondents were asked whether they used the same password for more than one Internet account. The results depicted in Table 3 display the responses for those respondents with two or more Internet accounts requiring passwords.

**Table 3** Repetition of passwords

| | **Repeating a password** | | **Using a variation of a password** | |
|---|---|---|---|---|
| Yes | 265 | 67% | 136 | 34% |
| No | 124 | 31% | 253 | 64% |
| | | | | |

| | | | | |
|---|---|---|---|---|
| Not answered | 8 | 2% | 8 | 2% |
| **Total** | **397** | **100%** | **397** | **100%** |

Of the respondents, 67% indicated that they used the same password to access other accounts, and 34% used a variation of a password to access another Internet account. This reinforces the finding that the respondents used similar passwords to access multiple Internet accounts.

One of the most basic requirements of good password practice is that the password should consist of at least eight characters (or considerably more) (Yan *et al.* 2004:28). With this in mind, students were asked to indicate the length of the password used to access their most frequently used Internet account. Of the respondents, 10% used passwords with fewer than six characters, 33% used passwords consisting of six characters and 15% had passwords with seven characters. Only 18% of the respondents had the minimum suggested number of characters of eight, while a further 16% indicated that their passwords had more than eight characters (7% of the students preferred not to answer this question). Of the respondents who answered this question, 63% employed passwords with fewer than eight characters. The average number of characters per password was 6,87, with a standard deviation of 2,27. This is in line with the findings by Riley (2006), who reported an average number of characters per password to be 6,84 (standard deviation of 1,79) in her study.

The type of account that arguably requires (in general) the use of a more secure password is Internet banking. The results for respondents who indicated Internet banking to be their most frequently used account showed that 47% of them used passwords consisting of eight or more characters. This was considerably more than the 37% of the total respondents who used eight or more characters for their passwords. However, more than 50% of the respondents still accessed their Internet bank accounts employing passwords with fewer than eight characters.

Another 'bad habit' noted in the password literature is writing down passwords (Adams and Sasse 1999:40–46; Barton and Barton 1984:186–194; Dhamija and Perrig 2000). In response to being asked whether they wrote down their passwords, only 36 (7%) of the respondents answered positively, 91% negatively, with 2% preferring not to answer the question. Only 38 students (7%) would give their password to somebody else. The result of this research does not support the concern of previous surveys (Adams and Sasse 1999; Barton and Barton 1984; Dhamija and Perrig 2000), with less than 7% of the respondents indicating that they wrote down or revealed their password to others in order to remember it.

A further control measure advocated in literature is that passwords should be changed regularly. The literature does not always agree on the specific period, but that it should be changed is a general recommendation. The students were asked how long they normally kept their passwords unchanged. They were also asked whether they would prefer to keep the password unchanged if they had the choice. Table 4 displays the results of this question.

**Table 4** Regularity of password change

| | | |
|---|---|---|
| Every two weeks | **7** | 1% |
| Every month | **30** | 6% |
| Every two to three months | **81** | 16% |
| Every six months | **29** | 5% |
| I never change the password on this account | **197** | 38% |

| | | |
|---|---|---|
| Only when prompted by the Web site to change my password | **155** | 30% |
| Not answered | **20** | 4% |
| | **519** | **100%** |

It appears that the discipline to regularly change passwords is lacking. Thirty-eight per cent never changed their passwords, with 30% doing so only when the Web site prompted them to change the password. In her survey, Riley (2006) reported that 52,7% of the respondents never changed their passwords when not required to do so. This is in line with our findings of 68% of the respondents who never changed their password except when prompted or required to do so by the system. This would mean that if the password was compromised, the account could be accessed for considerable periods of time, even *ad infinitum*. Respondents were also asked whether they would prefer to keep their password unchanged if they had the option. More than 71% of the respondents indicated that they would never change their passwords if given the choice.

One would expect that, when selecting a password, users will take into account the sensitivity of the information that will be exchanged when they access an Internet account. This survey confirms this notion in that 66% of the respondents indicated that they took the sensitivity of information to be communicated into consideration when selecting a password. Of the respondents, 57% indicated that they would make use of a stronger password when accessing these Internet accounts (e.g. Internet banking).

### 3.2 Knowledge and application of good password practice

A number of questions were designed to evaluate the students' perceptions and knowledge of good password practice, as well as how they applied their knowledge in creating passwords.

More than 69% of the respondents indicated that they were aware of what good password practices were. Of these respondents, the majority (63%) responded that this knowledge was at least partially based on general knowledge acquired through using the Internet, with 49% indicating that the knowledge was at least partially gained through university lectures. Their perceived knowledge was further assessed in subsequent questions in the survey.

The students were provided with a list of 20 possible practices that they could follow when selecting a password. They were asked to: (a) indicate which of the 20 possibilities they used when selecting a password; and (b) indicate which of the same 20 possibilities they considered to be good password practice. In both instances students were able to select all the applicable possibilities, resulting in the total being more than the number of respondents. In Table 5 there is a summary of the results that are sorted on the basis of the strength of the particular password practice.

**Table 5** Password practices in selecting a password: Use and good practices

| **Weak password practices** | **Use** | | **Good practices** | |
|---|---|---|---|---|
| Lowercase letters | 286 | 55% | 145 | 28% |
| Personally meaningful words (pets, street addresses) | 144 | 28% | 71 | 14% |
| Personally meaningful numbers (birthdates, phone numbers, etc.) | 120 | 23% | 62 | 12% |
| A standard word in ANY dictionary | 22 | 4% | 38 | 7% |

| | | | | |
|---|---|---|---|---|
| Names of friends, relatives | 96 | 18% | 37 | 7% |
| Same character three or more times | 16 | 3% | 37 | 7% |
| Geographical locations | 24 | 5% | 29 | 6% |
| A standard word in an Afrikaans or English dictionary | 32 | 6% | 21 | 4% |
| Simple sequence of characters (12345, qwerty) | 31 | 6% | 20 | 4% |
| Names of famous people | 16 | 3% | 12 | 2% |
| Your name/surname | 59 | 11% | 8 | 2% |
| Relate password to the Web site you are on | 7 | 1% | 8 | 2% |
| Login name (i.e. password is the same as username) | 18 | 3% | 7 | 1% |
| **Medium password practices** | | | | |
| Numbers or digits (e.g. 1, 2) | 287 | 55% | 245 | 47% |
| Standard words, but reversed (e.g. cat becomes 'tac') | 13 | 3% | 102 | 20% |
| Uppercase letters | 78 | 15% | 82 | 16% |
| **Strong password practices** | | | | |
| Numbers and special characters in place of letters (m@Tr!x) | 47 | 9% | 214 | 41% |
| Special characters (e.g. ^,%,$) | 36 | 7% | 213 | 41% |
| Capitalized word with numbers | 45 | 9% | 175 | 34% |
| Spaces | 27 | 5% | 145 | 28% |
| **Not answered** | 15 | 3% | 22 | 4% |

The students were generally able to identify which password practices were stronger than others, but for the most part they indicated that they did not apply their knowledge about strong passwords when creating a password. Differences between password practices that users reported and the password practices they believed they should use include the following:

- Of the students, 41% indicated that they knew that it was good practice to use a combination of letters, numbers and special characters in creating a password, but only 9% actually applied this when creating their password.
- Most respondents (74%) were aware that it was not good practice to use personally meaningful numbers, words, names of friends, etc. However, 54% of the respondents used personal information when selecting a password (i.e. personally meaningful words and numbers, names of friends or relatives, their own name or geographical locations), with 11% of the respondents using their own name as their password.
- Of the 59 respondents who indicated Internet banking as their primary Internet account, a worrying 59% used weak password practices. The security surrounding Internet banking passwords should be high, but 29 of these respondents (49%) used personally meaningful words or numbers, and six (10%) even used their own names or surnames as passwords. Of these 59 respondents, 68% were able to identify at least some of the more secure password practices, but only 41% applied these good practices.

The result of this survey reinforces the expectation that passwords are chosen so that they can be easily remembered (e.g. a meaningful word or number), and not necessarily on the basis of what is recommended as good and secure practice.

In spite of the fact that the results of the survey indicated that the passwords selected and

used by respondents are not necessarily of the highest standard, 75% of the respondents felt that their passwords were difficult to guess. This might show a high level of naïveté and a perception that 'it will never happen to me'. However, on the issue of whether they would be changing their passwords because they felt that they had learned something from the questionnaire, 190 (37%) of the respondents indicated that they would.

top

## 4 Discussion and conclusion

This survey indicates that a typical student at a South African university creates 1,8 passwords to access 3,2 Internet accounts, with the typical password used for about 1,7 accounts. The most common Internet accounts accessed by students that require passwords are e-mail, information-based accounts, Internet banking and other diverse accounts.

The majority of participants in this survey most commonly reported password generation practices that are simplistic and therefore very insecure. Particular practices reported include using lowercase letters, personally meaningful words and numbers. This includes birthdays, anniversary dates, telephone numbers, identity numbers, personal names, etc. that could be easily guessed with a basic knowledge of the respondent's interests. In this survey it was found that 43% of the respondents reported that they did not vary the complexity of their passwords to match the nature of the site, and 68% indicated that they never changed their password if they were not required to do so. When creating a password, more than 63% of the respondents used passwords that contained fewer than eight characters. However, hardly any of the respondents (less than 10%) wrote down or communicated their password to others in order to remember the password.

Previous research emphasizes the pervasive use of one's own name in password construction (Barton and Barton 1984:193; Brown *et al.* 2004:649; Harada and Kuroki 1996:32). However, in this survey only 11% of the respondents used their own names as passwords, compared to 42% as reported by Harada and Kuroki (1996), and 15% as reported by Brown *et al.* (2004:649). Other researchers have expressed concern about the dangers of re-using the same password (Adams and Sasse 1999; Dhamija and Perrig 2000), with the result of this survey revealing that password duplication is a very common practice.

The respondents in this survey professed to be knowledgeable in what constitutes good password practices, but were loath to make use of them, probably because to do so places an onerous duty on them to remember it. A reassuring finding is that students would not easily share passwords or write them down. More secure passwords are selected when the Web site contains more secure information, but passwords are generally rarely changed, which might reduce the effectiveness of any other security measures. Furthermore, students are aware of what constitutes good password practices when a password is selected, but do not employ these practices. The result of this study is in line with recent research that had similar findings, for example Riley (2006), Brown *et al.* (2004) and Yan *et al.* (2004).

The findings of this survey highlight the problem that information managers in general have in securing personal and financial information accessed through the Internet. The wide-spread reporting on identity theft, where unauthorized access led to the financial loss of users, and supplying of information and guidance on the proper selection and usage of passwords have not changed the behaviour of users dramatically. Although users in general are more aware of the dangers of selecting weak passwords, this survey indicates that users generally ignore this advice and still employ password practices that put them at risk. Information managers should therefore not rely solely on users to employ good password practices, but actively seek other means to enforce users to adhere to minimum password

practices (such as forced changes of passwords on a regular basis, minimum length of passwords, disallowing the re-use of old passwords, etc.). This study was performed with a population of students studying Information Systems. While it might be argued that these students would possess a high level of technological knowledge, it is clear from the results that this possible level of knowledge does not necessarily influence their behaviour. Users therefore might have the knowledge required for good password practices, but do not necessarily apply this knowledge in practice.

These are matters to be taken into consideration when any information is to be secured by making use of passwords. Users tend not to use secure passwords or password practices and limited faith should be placed on these practices. When creating a password to access an Internet account, users should first differentiate between those accounts where security is genuinely important and those where a breach of security would not constitute an important informational or financial compromise. Where security needs are minimal, a common password that is easy to remember may be used. Where security is essential, a stronger password should be used.

Furthermore, when organizations allow users access to sensitive information, information managers should be aware of the practices users employ when creating and using passwords. Where security is essential, users should be forced by the system to comply with good password practices by, for example, determining the minimum number of characters that a password should consist of and requiring at least a combination of numbers, letters and special characters or spaces, as well as that the user should be forced to change the passwords regularly. Users should also be continually informed regarding the vulnerability of password-protected systems.

The results of this survey highlight the current practices employed by users when creating and using passwords to access information. Organizations and information managers cannot rely only on users to employ proper password control in order to protect sensitive information. It may be essential for organizations to set up the information system to enforce good password practice and to continually make users aware of the dangers of identity theft if users do not employ good password practices.

top

## 5 References

Adams, A. and Sasse, M.A. 1999. Users are not the enemy; why users compromise computer security and how to take remedial measures. *Communications of the ACM* 42(12):40-46.

Andrews, L.W. 2002. Passwords reveal your personality. *Psychology Today* 35:12-20.

Armstrong, L. 2002. And the password is …#%?@&!. *Business Week* 3 June 2002. [Online]. Available WWW: http://www.businessweek.com/magazine/content/02_22/b3785119.htm (Accessed 23 January 2007).

Barton, B.F. and Barton, M.L.S. 1984. User-friendly password methods for computer-mediated information systems. *Computers & Security* 3:186-195.

Bishop, M. and Klein, D.V. 1995. Improving system security via proactive password checking. *Computers & Security* 14:233-249.

Brown, A.S., Bracken, E., Zoccoli, S., Douglas, K. 2004. Generating and remembering passwords. *Applied Cognitive Psychology* 18(6):641-651.

Butler, R. 2005. Avoid the hook in the phisherman's bait. *Accountancy SA* August 2005:16-18.

Davis, C. and Ganesan, R. 1993. BApsswrd: A new proactive password checker. *Proceedings of the National Computer Security Conference 1993, the 16 th NIST/NSA conference* 1-15.

Dhamija, R. and Perrig, A. 2000. Déjà vu: a user study. Using images for authentication. In: *Proceedings of the 9 th USENIX Security Symposium*, Denver, Colorado, USA, August 2000. [Online]. Available WWW: http://www.usenix.org/events/sec2000/dhamija.html (Accessed 18 January 2007).

Gheringer, E.F. 2002. Choosing passwords: security and human factors. *Proceedings of IEEE 2002*:369-373. [Online]. Available WWW: http://research.csc.ncsu.edu/efg/ethics/papers/passwords.pdf (Accessed 4 January 2007).

Harada. Y., and Kuroki, K. 1996. A study on the attitude and behaviour of computer network users regarding security administration. *Reports of National Research Institute of Police Science* 37:21-33.

Kaye, D. 1995. The importance of information. *Management Decision* 33(5):5-12.

Proctor, R.W., Lien, M.C., Vu, K.P.L., Schultz, E.E. and Salvendy, G. 2002. Improving computer security for authentication of users: influence of proactive password restrictions. *Behaviour Research Methods, Instruments & Computers* 34(2):163-169.

Riley, S. 2006. Password security: what users know and what they actually do. *Usability News* 8(1). [Online]. Available WWW: http://psychology.wichita.edu/surl/usabilitynews/81/Passwords.htm (Accessed 4 January 2007).

Schneier, B. 2004. Customers, passwords and Web sites. *IEEE Security & Privacy* July/August. [Online]. Available WWW: http://www.schneier.com/essay-048.html (Accessed 4 January 2007).

Vu, K.P.L., Bhargav, A. and Proctor, R.W. 2003. Imposing password restrictions for multiple accounts: impact on generation and recall of passwords. *Proceedings of the 47 th annual meeting of the Human Factors and Ergonomics Society*. Santa Monica:1331-1335.

Weinshall, D. and Kirkpatrick, S. 2004. Passwords you'll never forget, but can't recall. *CHI* April 2004: 24-29. [Online]. Available WWW: http://www.cs.huji.ac.il/~kirk/Imprint_CHI04_final.pdf (Accessed 5 January 2007).

Yan, J., Blackwell, A., Anderson, R. and Grant, A. 2004. Password memorability and security: Some empirical results. *IEEE Security & Privacy* September/October 2004:25-31. [Online]. Available WWW: http://ieeexplore.ieee.org/iel5/8013/29552/01341406.pdf?arnumber=1341406 (Accessed 5 January 2007).

top

**Disclaimer**

or the Rand Afrikaans University. The user hereby waives any claim he/she/they may have or acquire against the publisher, its suppliers, licensees and sub licensees and indemnifies all said persons from any claims, lawsuits, proceedings, costs, special, incidental, consequential or indirect damages, including damages for loss of profits, loss of business or downtime arising out of or relating to the user's use of the Website.

ISSN 1560-683X

Published by InterWord Communications for Department of Information and Knowledge Management, University of Johannesburg