ORIGINAL ARTICLE

A SURVEY ON COMPUTER PASSWORD PRACTICES AMONG MEDICAL UNDERGRADUATE STUDENTS AT FACULTY OF MEDICINE, NATIONAL UNIVERSITY OF MALAYSIA

M T Azmi [1] and M T Emran [2]

[1] Department of Community Health, Medical Faculty,Universiti Kebangsaan Malaysia and [2] Department of Computer and System Technology, Faculty of Computer Science and Information Technology,Universiti Malaya

ABSTRACT

Background: *Without any doubt, the combo of user ID and password are the most used authentication method in the computing and internet environment. However, due to the enormous number of accounts that require password authentication, users tend to develop bad habits in their password practices which in turn will put their account security at risk. With the increasing use of computing in health-care settings and the use of EMR in hospitals, such practices are a cause for concern.*

Methods: *This is a cross-sectional study using self-administered questionnaires, investigating the practice of the respondents in keeping their passwords secure. Respondents in this survey are the undergraduate students of Faculty of Medicine, Universiti Kebangsaan Malaysia.*

Results: *Among the findings are that 87.4% of the respondents used the same password for more than one account. If a user used the same password for several accounts, it might trigger a domino effect if any of the account passwords were compromised. A total of 98.9% of the respondents memorised their password only in their mind, without writing down the password anywhere. This may lead to using easily guessable passwords which may introduce additional security risk to their accounts. The majority of the respondents (96.6%) never or rarely change their passwords. The study also showed that 82.7% of the respondents used passwords which are 6-8 characters in length. Longer passwords are usually safer but harder to remember. The questionnaire also explored the users' password combination style, whether they used numbers only or combination of numbers and alphabets or some other pattern. A total of 39.1% used letters only but 27.6% used combination of numbers only which is less secure. About 77% of the respondents used personal information such as their birthday date or a person's name as part of their password.*

Conclusions: *This habit may make their password guessable to people who are close to them. In conclusion, most medical students are not practising safe password conduct and they should be educated on this. If not, patients' data confidentiality may be compromised in the future due to such practices.*

Keywords: *EMR security, computerised medical system security, password practice*

INTRODUCTION

The forthcoming wide availability of high bandwidth internet connection combined with mass computer system have paved the way for the rise of computerised health care services which include mobile health services [1], web-based telemedicine, videoconferencing for remote consultation [2], world-wide observation of diseases, distance surgery and even distance learning in medical education [3]. The world of health care is on its way to be transformed by the advent of more integrated and powerful IT-systems [3, 4]. Even nowadays, many hospitals utilise combinations of mainframes and PC-based local area networks which together form large, distributed information and communication systems [3].

Correspondence to: M T Azmi, Department of Community Health, Medical Faculty,Universiti Kebangsaan Malaysia
Tel: 03-91702527, Fax: 03-91737825
(e-mail: drtamil@medic.ukm.my)

Among the main motivation which accelerates this growth is that the effectiveness and service quality in a medical environment can be improved by using electronic documents to speed up both doctors' activity and administration. Computerised system provides easy retrieval and use of needed data without losing the convenience [5]. The efficiency of modern health care has now relies more upon a computerised infrastructure [6].

The rise of computer based system usage in medical organization has increase the need of digital security. Security features must be upheld when a completely digitalized system is used [5]. For example, the integrity of medical data in storing, processing and transmitting must be preserved to prevent undetected, unauthorised modification of the data [7]. It will be a disastrous if a critical medical IT-systems which is relied upon by health professionals in their clinical work, fails in terms of integrity or accuracy [6, 8].

This scenario has put security as among the priority requirement in developing medical system. The Swedish project SITHS (Secure IT within Health Care) which is a collaboration to develop models and methods for basic security functions required when using IT-support for the health care, has suggest several functions to be implemented.

Among them are [7];

- Control of given identity;
- Establishment of access rights;
- Protection of information against inappropriate insight;
- Protection of information against undesired change;
- Protection against afterward denial of sender or receiver of information concerning action or knowledge about action;
- Functions for traceability.

Security was also one of the major requirements taken into consideration in Advanced Interactive Digital Administration (AIDA) system's design which is used in several medical system [5]. Another project, called Mobihealth implement several security and communication technologies such as IP Security (IPSEC), Secure Sockets Layer (SSL), Hypertext Transfer Protocol over Secure Socket Layer (HTTPS), JINI and Remote Method Invocation (RMI) [9].

However, no matter how much attention and consideration given to ensure security in any computerised medical system, human factor are more important as human has always been the weakest link in security management. It is important that human beings that uses and administers the computerised medical system to practice good security policy to ensure the system integrity are upheld. For example, there is no security in a system that implements state-of-the-art security system if the administrator sets a blank password to access the system. Therefore, this paper investigates one aspect of human error factor in security which is the attitude in managing password as the combo of user ID and password are the most used authentication method in the computing and internet environment. The new hospital information system in Universiti Kebangsaan Malaysia Hospital (HUKM), known as c-HETS also ultilises the username-password combo for system security. Due to the enormous number of accounts that require password authentication, users tend to develop bad habits in their password practices which in turn will put their account security at risk. With the increasing use of computing in health-care settings and the use of EMR in hospitals, such practices are a cause for concern.

METHODS

This is a cross-sectional study using self-administered questionnaires. It investigates the practice of the respondents in keeping their passwords secure. Respondents in this survey are the year two undergraduate students of Faculty of Medicine, Universiti Kebangsaan Malaysia. The survey questions are divided into two parts. The first part of the questionnaire investigates basic background of the respondent like their age, gender, experience using internet and internet usage frequency.

The second part of the survey probes the password practices of the respondent. It began with questions probing how many password protected accounts do they have. Then this section continues with questions investigating whether the users utilise practices which are regarded as vulnerable and introduce risk to their password protected account.

Among practices investigated were;

- Did they use the same password for more than one account?
- Did they fully memorised their password or they wrote it somewhere?
- And do they frequently change their password?

The questionnaire also checks the content of the password as it is also a very important aspect of their password security. For example the questionnaire checks whether they used personal information as a part of their password like their birthday, favourite celebrity, favourite idol, hobby, place of birth or whether any of the words in their passwords can be found in any dictionary of any language.

A pilot test was carried out before the questionnaires were distributed to the target respondents. The first draft was completed by ten students. The test concentrates on the ease of understanding the questions, the suitability of the questions flow and the appropriateness of the questions wording and answers option. Based on the feedback, some amendments were made to the first draft.

The modified questionnaires were then distributed randomly among year two undergraduate students of Medical Faculty, National University of Malaysia. From the 100 questionnaires distributed, 87 respondents returned the completed questionnaire and their responses were used for this study.

RESULTS & DISCUSSION

Table 1: Socio-Demographic Profile Of Respondents

Factors	Categories	Frequency	%
Age	19	5.0	5.7
	20	60.0	69.0
	21	20.0	23.0
	22	1.0	1.1
	29	1.0	1.1
Gender	Male	48.0	55.2
	Female	39.0	44.8

Since the study was conducted among year two medical students, the respondents were of similar age. A total of 55.2% respondent were males and 44.8% were females.

How many accounts that require an id and password do you have?

A total of 37.9% of the respondents have 3-5 accounts while another 24% have 6-10 accounts. Current trend requires us to have more accounts for daily use (i.e. email/online banking/computer login). The more accounts we have, the more login passwords we need to remember. Huge number of accounts held by the user is identified as a major factor contributing to insecure password practice by several researchers. Logging in with usernames and passwords has become one of the most ubiquitous and most common rituals of the Internet age [10]. Users are often asked to generate, memorize, and keep secret a growing number of passwords as they join new password protected sites from time to time

Table 2: Number of accounts and passwords of respondents.

Factors	Categories	Frequency	%
Number of accounts	1	14.0	16.1
	2	15.0	17.2
	3	14.0	16.1
	4	9.0	10.3
	5	10.0	11.5
	6	7.0	8.0
	7	7.0	8.0
	8	2.0	2.3
	9	3.0	3.4
	10	2.0	2.3
	11	1.0	1.1
	12	1.0	1.1
	13	1.0	1.1
	15	1.0	1.1
Uses the same password	No	10.0	11.5
	Yes-most	45.0	51.7
	Yes-several	17.0	19.5
	Yes-few	13.0	14.9
	Yes-other	1.0	1.1

Have you ever used the same password for more than one account?

A total of 87.2% respondents admitted that they were using the same password for more than one account. This trend could increase as the number of account per person that requires a password authentication increases. If a user used the same password for several accounts, it might trigger a domino effect if any of the account passwords were compromised. A hacker gaining access to one account may be able to gain access to the others account [11]. Lu & Twidale [12] wrote that in an effort to combat login name and password overload, users have devised their own solutions like writing down passwords, using the same login and password for all their accounts and when forced to change their passwords at intervals, they adapt by making simple, easily guessable changes.

How do you memorise your password?

In memorising their password, 86.2% respondent said they only memorised the password but another 12.6% respondent said they used easily guessable password. Human beings have a strong tendency to choose relatively short and simple passwords that they can remember and they will often choose the simplest password possible or common words and names [13].

Table 3: Password Habits Of Respondents

Factors	Categories	Frequency	%
Memorises password	Easy guessable	11.0	12.6
	Memorised	75.0	86.2
	Other	1.0	1.1
Frequency of password change	1-3 months	2.0	2.3
	3-6 months	1.0	2.1
	Don't know/rarely/never	84.0	96.6
Password format	letters	34.0	39.1
	letters & numbers	23.0	26.4
	letters, numbers & ASCII characters	3.0	3.4
	letter (upper/lower)	1.0	1.1
	letter (upper/lower) & numbers	1.0	27.6
	numbers	24.0	27.6
	others	1.0	1.1
Password available in dictionary	No	69.0	79.3
	Yes	18.0	20.7
ATM pin as password	No	67.0	77.0
	Yes	20.0	23.0
Sharing password with others	No	54.0	62.1
	Yes	33.0	37.9
Know password of others	No	49.0	56.3
	Yes	38.0	43.7
Think that password is safe	No	29.0	33.3
	Yes	58.0	66.7

How do you memorise your password?

In memorising their password, 86.2% respondent said they only memorised the password but another 12.6% respondent said they used easily guessable password. Human beings have a strong tendency to choose relatively short and simple passwords that they can remember and they will often choose the simplest password possible or common words and names [13].

How frequent do you change your password?

It is advisable for a user to change their password after a certain period to ensure higher security but 96.6% of the respondent rarely/never changed their password which is an alarming situation.

What kind of password describes your password format the best?

On selecting password format, the best advisable password format is the one that combines letters (upper & lower case), numbers and special character but only 3.4% respondent use this format. Another 27.6% of respondents use numbers only, which is deemed as insecure as any automated password breaker software could easily break such a password.

User may also use some personal info as whole or part of their password. This includes special numbers (birthday, anniversary), special person (artist, lover, or politician) or special hobby/interest (car, colour, or food). While this may enable the user to easily recall their password, other people that are close to the user or know much about the user may be able to correctly guess the password. A total of 77% of the respondents said that they used personal info as whole/part of their password. Using personal information in a password introduce risk to the user's account. Good password choice should avoid common words and names [14].

Can any of your passwords be found in any dictionary of any language?

A total of 20.7% of the respondents said their password can be found in the dictionary. Practices of using words that can be found in any dictionary of any language which include common words make the key or password search job a lot easier [13]. Using password that can be found in dictionary is quite dangerous as password breaking software could easily break this type of password.

Do you use your ATM bank card pin number as password for any of your accounts?

A total of 23% of the respondent said that they used their ATM pin number as their password. This introduces a great risk whereby if their password were compromised, their ATM pin may also be compromised. Person who may have access to their password might try to obtain their ATM card for unauthorised use.

Have you ever shared any of your account passwords with anyone else? Do you know password for any account that does not belong to you?

A total of 37.9% of the respondent said they have shared their password with someone else while 43.7% respondent said they know password that does not belong to them. Users have developed a habit of sharing their password. This habit exposes their password and risk being compromised or misused.

Do you think your password is safe?

In the last question, respondent are asked whether they think their password are safe. A total of 66.7% of the respondents think that their password is safe while another 33.3% of the respondent think otherwise.

CONCLUSION

This survey shows that most of the year two undergraduate students of Faculty of Medicine, Universiti Kebangsaan Malaysia do not practise safe password practices. With the increasing use of computing in health-care settings and the use of Electronic Medical Record (EMR) in hospitals, such trends are a cause for concern. As more hospitals and health organisations use computer based software which contain sensitive information & critical function, medical student should be educated to ensure they practise secure password practices. This is to ensure the security and safety of the system and organisation are not jeopardised by such bad practices.

REFERENCES

1. Richard Bults, Katarzyna Wac, Aart Van Halteren Dimitri Konstantas, Val Jones, Ing Widya. 2004. "Body Area Networks for Ambulant Patient Monitoring Over Next Generation Public Wireless Networks" *In Proceedings of 3rd IST Mobile and Wireless Communications Summit*, 2004.
2. Chen, Z., Yu, X., and Feng, D. 2001. Telemedicine system over the internet. *In Selected Papers From the Pan-Sydney Workshop on Visualisation - Volume 2* (Sydney, Australia). P. Eades and J. Weckert, Eds. ACM International Conference Proceeding Series, vol. 9. Australian Computer Society, Darlinghurst, Australia, pp. 113-118.
3. Gerrit Bleumer. 1997. "Cryptographic Mechanisms for Health Care IT-Systems" in Barry Barber, Kees Louwerse, Alison Treacher (eds.): Towards Security in Medical Telematics: Legal and Technical Aspects, SHTI Vol 27, IOS-Press, Amsterdam 1996, pp. 233-237
4. Rienhoff O.. 1994."Digital archives and communication highways in health care require a second look at the legal framework of the seventies", *International Journal of Biomedical Computing*, 1994, Feb (35), (Suppl), pp. 13-19.
5. Diana Berbecaru, Antonio Lioy, Marius Marian. 2002. "Secure Digital Administration In Medical Environment" in

Proceedings of IADIS International Conference WWW/Internet 2002.
6. Gerrit Bleumer. 1995. “Secure Environment for Information Systems in MEDicine:SEISMED(A2033)”, Technical Report, AIM (Advanced Informatics in Medicine),1995.
7. Gerrit Bleumer. 1994, “Security for Decentralized Health Information Systems” *International Journal of Biomedical Computing*. 1994 Feb (35) (Suppl) pp. 139-45
8. Neumann PG. 1995. Computer Related Risks; *ACM Press*, Addison Wesley, Reading Massachusetts 1995.
9. Ramon Martí & Jaime Delgado. 2003. “Security in a Wireless Mobile Health Care System”, *In Proceedings of MobEA (Emerging Applications for Wireless and Mobile Access)*, 2003.
10. Halderman, J. A., Waters, B., and Felten, E. W. 2005. “A convenient method for securely managing passwords”. *Proceedings of the 14th international Conference on World Wide Web*, Chiba, Japan, 10-14 May 2005, pp 471-479. ACM Press.
11. Ives, B., Walsh, K., & Schneider, H.. 2004. “The domino effect of password reuse”, *Communications of the ACM*, *47* (4), pp. 76-78.
12. Lu, B. & Twidale, M.B.. 2003. Managing Multiple Passwords and Multiple Logins: MiFA Minimal-Feedback Hints for Remote Authentication. *Proceedings of Interact 2003*, Zurich, pp. 821-824, IOS Press.
13. Morris, R., & Thompson, K. R.. 1979. Password Security: A Case History. *Communications of the ACM*, *22* (11), pp. 594-597.
14. Spafford, E.. 1992. OPUS: Preventing weak password choices. *Computers & Security* 11, (2), Elsevier.