Artículo de investigación

Evaluation of Password Pattern Used by the Students of Health Information Technology

Evaluación del patrón de contraseña utilizado por los estudiantes de tecnología de la información de salud

Avaliação do Padrão de Senha Utilizado pelos Alunos de Tecnologia da Informação em Saúde

Recibido: 16 de enero de 2019. Aceptado: 06 de febrero de 2019

Written by:
Somayeh Niazi Kaji[62]
Amir Jamshidnezhad*[63]
Ali Talebi Shoushtarian[64]

Abstract

Today, technology is used as an important and foremost tool to facilitate human life. Computers, tablets, smart phones and massive social networks have affected the health and medical professions. Keeping security in such environments is one of the important and critical issue. Choose of a proper password for user accounts is a challenging matter for security in the digital environment. This study was conducted to consider the authentication level for the academic users. The sample size was found using the Gregis Morgan formula. Therefore, the patterns of passwords used in cyber environments by 200 students of IT Sciences were investigated and considered. Descriptive statistics have been used to analyze the gathered data in this study. The results showed that the passwords selected by the students were poor and imaginable for breaking.

Keywords

Password patterns, Authentication, Attack patterns, Security of account, Information Technology.

Resumen

Hoy en día, la tecnología se utiliza como una herramienta importante y principal para facilitar la vida humana. Las computadoras, tabletas, teléfonos inteligentes y redes sociales masivas han afectado a la salud y las profesiones médicas. Mantener la seguridad en tales entornos es uno de los temas importantes y críticos. La elección de una contraseña adecuada para las cuentas de usuario es un tema difícil para la seguridad en el entorno digital. Este estudio se realizó para considerar el nivel de autenticación para los usuarios académicos. El tamaño de la muestra se encontró utilizando la fórmula de Gregis Morgan. Por lo tanto, se investigaron y consideraron los patrones de contraseñas utilizadas en los entornos cibernéticos por 200 estudiantes de ciencias de TI. Se han utilizado estadísticas descriptivas para analizar los datos recopilados en este estudio. Los resultados mostraron que las contraseñas seleccionadas por los estudiantes eran deficientes e imaginables para romperlas.

Palabras clave

Patrones de contraseña, Autenticación, Patrones de ataque, Seguridad de cuenta, Tecnología de la información.

[62] Department of Health Information Technology, Faculty of Medicine, Ahvaz Jundishapur University of Medical Sciences, Ahvaz, Iran

[63] Department of Health Information Technology, Faculty of Medicine, Ahvaz Jundishapur University of Medical Sciences, Ahvaz, Iran. (Corresponding Author)

[64] Department of Medical Library and Information Sciences, Faculty of Allied Health Sciences, Ahvaz Jundishapur University of Medical Sciences, Ahvaz, Iran

Resumo

Hoje, a tecnologia é usada como uma ferramenta importante e importante para facilitar a vida humana. Computadores, tablets, smartphones e grandes redes sociais afetaram as profissões médicas e de saúde. Manter a segurança nesses ambientes é uma questão importante e crítica. A escolha de uma senha adequada para contas de usuário é um assunto desafiador para a segurança no ambiente digital. Este estudo foi realizado para considerar o nível de autenticação para os usuários acadêmicos. O tamanho da amostra foi encontrado usando a fórmula de Gregis Morgan. Portanto, os padrões de senhas utilizados em ambientes cibernéticos por 200 estudantes de Ciências da TI foram investigados e considerados. Estatísticas descritivas foram utilizadas para analisar os dados coletados neste estudo. Os resultados mostraram que as senhas selecionadas pelos alunos eram ruins e imagináveis para quebrar.

Palavras-chave
Padrões de senha, autenticação, padrões de ataque, segurança da conta, tecnologia da informação.

Introduction

Considering the importance of information technology (IT) in the present era and the rapid and yet uneven growth of IT structure make it potentially vulnerable to threat the personal life (1).

In recent decades, computer and network security has been identified as a technical problem. A key issue in future security research is authentication, which indicates whether a user can have access to the information source. Password is one of the usual mechanisms that is always used for the authentication systems (2). Therefore, the first step of security in the cyber environment is to have a strong password. Password patterns are affected with the risk of crack and failing from the mind. Passwords are an important part of the security and confidentiality of information and are in fact at the forefront of protecting user accounts (3).

Confidentiality means that unauthorized persons are denied to access to the stored and exchange electronic data (4). Moreover, Security includes the actions, techniques and technologies used to protect information as well as accountability (5).

Researcher found that a password may be secured if at least includes the following factors:

1- Minimum 12 characters
2- A combination of numbers, symptoms, and small and large symbols
3- Not a meaningful word or a combination of a meaningful words
4- Replaced and obvious characters not be used (6).

The topic of considering password patterns is always attractive and interesting to determine the methods of choosing passwords. However, research still show the limitation of the studies in the field of considering the password patterns (3). In the past decade, a new interest in the use of graphical passwords has been created as a substitute for text-based passwords among users due to more secure condition against the attack methods. However, the text password patterns are still popular by the users (7). A study conducted by Maurice and Thompson (8) showed that over 86% of 3286 users used the poor security patterns.

A study on data extracted from the database of Sony Company showed that more than 67% of users used the similar password pattern for their various user accounts (9).

Moreover, recent studies considered the user's habits to create the password patterns existed in the MNS, Paypal, NyTimes databases (10). Research showed that there were not absolute security in the created passwords, however, the level of security is almost acceptable for the users according to their secure requirements (1). Asadi et al (11) showed that a combination of fingerprints and one of the user's personal characteristics as a more protected method than a single pattern was greatly increased among the users (11). In a study by Heidary and Ahmadzadeh (12), the mouse was used to enter the password, in which the pixels of the password were composed of the output. This method protected the user's password against disclosure. In this method, when the user entered the password with the mouse, the user's

password was replaced with the value of the password matrix.

The present study was carried out to investigate the pattern of passwords selected by university students to find the security level of user accounts.

Materials and methods

The population of this study consisted of Health Information Technology students. Sample size was determined using the Grizzly Morgan formula. Also, a checklist was used to collect data regarding to password patterns used by the students. The reliability of the checklist was assessed by two experts in the field of IT. The checklist included three parts to find the security information regarding to accounts for students academic profiles, email and mobile phones. According to sample size, 200 samples were cooperated in the study. Data analysis was carried out using descriptive statistics by SPSS version 22 software.

Results

Findings regarding to the pattern of email passwords are shown in Table 1. According to Table 1, 26.1% of the students used a specific number for their email password and 21.53% used a combination of numbers and characters. Most of the samples suggested to use not weak security level for their e-mail accounts.

Table (1) Proportion of Password Patterns in Email Accounts

Password patterns options	Proportion	Frequency
A specific number	26.1%	51
Combine numbers and characters	21.53%	42
National ID number	15.38%	30
Other numbers	15.38%	30
Year of Birth	7.69%	15
Name of a specific person	7.17%	14
Name of a specific things	6.66%	13
A set of letters	5.12%2	10
Student number	3.58%	7
Characters	1.58%	3

Table 2 shows the results of investigating the student academic accounts security patterns. According to Table 2, around 71.28% of the students used the national ID number for their account as the first patterns. However, 9.74% of users used their passwords to the years of birth. A specific name was the less patterns used for the academic accounts.

Table (2) Proportion of Security Patterns in Students' Academic Accounts

Password patterns options	Proportion	Frequency
National number	71.28%	139
Year of Birth	9.74%	19
Student number	7.69%	15
Other numbers	6.66%	13
A specific name	4.61%	9

Table 3 shows the results of considering the patterns of mobile phones passwords. According to Table 3, 44.61% of students used the graphical patterns for their mobile phone password. Moreover, 28.20% of them used a specific number for their accounts. However, name of the specific persons were not included in their selected options.

Table (3) Proportion of Security Patterns in Students' Mobile Accounts

Password patterns options	Proportion	Frequency
Graphical Patterns	44.61%	87
Specific number	28.20%	55
Other numbers	7.17%	14
Year of Birth	6.15%	12
Combination of number and characters	5.12%	10
A specific name	4.10%	8
A set of letters	2.16%	5
Student number	1.02%	2
National ID number	0.5%	1
Characters	0.5%	1
Name of a specific person	0%	0

Discussion

Passwords pattern is still one of the most important issues for protecting the privacy of individuals. Increasing the number of accounts in different applications is led to use similar passwords by the users for their accounts. A password has appropriate security level if includes the following parameters:

1- Minimum 12 characters
2- A combination of numbers, symptoms, and small and large symbols
3- Not a meaningful word or a combination of a meaningful words
4- Replaced and obvious characters not be used (6).

In study by Mousavi et al (2), email attachments were considered as the most important attack methods. So, the users have the right policies to select strong passwords to decrease the risk of these attacks. In this study, over than 21% of the students used the combination of numbers and characters for their email accounts. However, this hybrid pattern was selected in a limit cases as a secure password pattern among the students. Therefore, email accounts with higher secure had more security importance in comparison with other accounts in this study. Moreover, national ID numbers as well as year of the birth were the other popular options used for the security of the accounts. It means, although the familiar IDs are not completely secure but the IT students preferred to use those patterns due to afraid of the forgetting. Year of the birth as well as the national ID number were used frequently not only in the email accounts but also in the Student's academic accounts and mobile accounts. National IDs and years of birth with 71.28% and 9.74% were the most used patterns for the students' academic accounts, respectively. Academic accounts showed less security importance than email accounts due to less accessibility and risk of those accounts on the web. Most frequency patterns in the mobile accounts was belonged to the graphical patterns. Graphical security patterns are the special security passwords in the mobile phones which not existed in other studied applications in this research. Those are easy to use and keep in the mind for users while are not as secure as input digit patterns. Therefore, mobile companies are working to find more secure methods such as biometrics than classical ways to increase the privacy of the mobile devices.

Generally, according to four security factors listed above, the studied accounts did not followed of those options in terms of most items of the given instruction. Therefore, more educational information about the risk of low security passwords for the students is recommended.

Conclusion

In this study, students' password patterns were considered for security in the accounts of email, academic profiles as well as mobile phones. The results showed that the passwords selected by the students were poor and imaginable for breaking. In such a way that many selected passwords contained personal information of individuals. Therefore, students are advised to regularly change their passwords and follow the security instructions to avoid of illegal accessibility to personal information.

References

1- Sohrab, S. Ahsan, R. Faqih Mirzaee, S. 2014, Comparison of demographic and password individual using data mining in organization, case study IT institute of excellence Qom, the first congress of new technologies to achieve sustainable development, institution of higher education Mehr Arvand.

2-Qochani, M.M. Mosavi, A. Hosseinpor, D. 2015, Protection and security of information By providing a conceptual model of social engineering, journal of security information imam hossein computer sieve university of tehran;3(14):65-84.

2-Mousavi, M.A. Moshiri, M.E. 2014, Combining authentication methods for mobile transactions, National conference on new achievements in science, engineering and basic electronics, Islamic Azad University of Boroujerd, Amir Kabir University of Tehran.

3-Arian, P. Tabakhi Faryzany, S.R. 2015, Quality field study and how to choose passwords between users in Iran, second international congress of technology, connection and knowledge(ICTCK2015),Mashhad, Islamic azad university of Mashhad.

4- Nayeb, N. SHarifi, Y. 2012, Providing a safe method to create a single password OTP by using mobile phone, Iran mobile congress, Tehran, Sharif university of technology research center.

5- Karami, M. Safdari, R. Soltani, A. 2013, Patient right Information: Guidelines for the Security Information In the electronic environment. Journal of Medical Ethics.7 (25):83-96.

6- Asadi Zangeneh, M. Asadi Zangeneh, S.H. Pour Normandy, R. 2014, Presentation a combination of fingerprint and personal information using fuzzy logic to increase the security and user identity system in ATM system, National conference on computer engineering and information technology management. Tehran, company farzin Sunrise Science & Technology.

7- Norizadeh, J. 2012, Check user authentication through graphic password, First national conference on information and network technology university Payamnor, Tabbas, Iran.

8- Marris, R. Thompson, K. 1979. Password security: case history. Comm. ACM,

9-http://www.pcmage.com/article 2/0,2817,2386533,00.asp 2014.11.21

10- Florencio, D. Herley, C. 2007, A large-scale study of web password habits. Proceeding of the 16th international conference on World Wide Web. ACM.

11- Zamani Babgohari, E. Elahizade Mahani, N. 2013, Checking administrative bodies of security problems in Iran and solution by with introduction of the software password security, first national conference on emerging trends in computer engineering and data recovery Rodsar, Islamic Azad university Rodsar, Iran.

12- Heidary, M. Ahmadzadeh, M. 2013, New ways of using password authentication pattern, second national computer conference, sanandaj,vocational school samai sanandaj.