www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 8 Issue 4 April 2019, Page No. 24586-24602
Index Copernicus Value (2015): 58.10, 76.25 (2016) DOI: 10.18535/ijecs/v8i04.4304

Evaluating Passwords User Behavior and the Psychology of Password Management

Walid Ali Sulaiman Ali Alothman

The Public Authority for Applied Education and Training (PAAET)
College Of Business Studies
Computer Science and Information System Department
Aladailiy Area., Block No: 4
P.O. Box: 23167, Zip-Code: 13092 State of Kuwait

Abstract
Regardless of how complex an association's security framework is, it stays helpless because of the human factor. Content based passwords are usually utilized for verification in figuring condition. Despite the fact that passwords are considered as the underlying line of assurance for users, they stay simple to compromise. To improve the security of frameworks, different password synthesis policies are embraced. These strategies guarantee that users are made to pick solid passwords that assistance anticipate online ruptures and information spills. Be that as it may, it likewise make passwords hard to retain and review, diminishing the general ease of use. In this examination we researched the ease of use of password strategies and users' view of password security. We additionally reviewed and examined the patterns practiced by users while producing passwords (Crantor, Hong and Reiter, 2016).

Users are not as mindful of security prerequisites and practices as they think. By far most of users' passwords are breakable within days or shorter. Strikingly, we found that the utilization of numbers and uppercase letters is common among clients. Numbers are generally utilized toward the end of the passwords and uppercase letters are for the most part utilized toward the start of passwords. The presence of such patterns makes it simpler for attackers to create progressively compelling dictionaries. In light of the examination in this investigation, we make suggestions to the IT office to improve the password policy (Shen, 2016).

Keywords: password management; password usability; password security; password behavior; password policies; user password

The Subject of the Study

In this study, we reviewed and dissected the examples rehearsed by users while producing passwords. We led a user study about dependent on test assessment and online overview. Amid the trial assessment users were approached to set their passwords utilizing four distinct passwords policies. We utilized numerous investigation setups and situations to make genuine circumstances. The outcome features the key difficulties faced by the users in reviewing complex passwords and their tendency towards setting easy-to-figure passwords.

The Aim of the Study

The investigation demonstrates that mind boggling password policies are irritating for users and it requires greater investment to make such passwords. Also, to build the memorability of passwords majority share of users pick relative names and normal dictionary words in their passwords. Utilizing same passwords for numerous accounts was likewise a typical practice seen amid the investigation. We additionally assessed the opposition of passwords made by the users against prominent assaults utilizing different password breaking devices.

Methodology

We propelled an intentional poll to give some knowledge into the password propensities for the users. The poll was direct and accumulated general data about the users and their picked passwords. The inquiries expected to discover the password length; the utilization of uppercase letters, special characters and digits; and the situation of these less usually utilized characters. We led an online review to assess our hypothesis.

Hypotheses

To comprehend the connection among convenience and security of passwords, we define eight hypotheses:

1. User Reuse same password for different records with little change.
2. Very few users know about the way that utilizing same password diminishes the security.
3. Computer alumni/PC educated users know the way that reusing same password reduce password security yet at the same time they reuse a similar password.
4. Mostly users use dictionary word, their own data, expressions and regular names as their password.
5. Complex passwords made utilizing secret key approaches are hard to retain and recall.
6. The strategies which are progressively entangled take additional time by user to create password.
7. Different age groups have distinctive kind of passwords.
8. Password meter help users to make better passwords.

Introduction

The present web influences an ever increasing number of parts of our lives at work and at home, from data inquiry and correspondence, to banking and venture. All things considered, online security has turned into an imperative administration issue for organizations, computer users, and society all in all. An online security break can prompt vast misfortunes. Indeed, even view of powerless online security can have negative results. Persistent checking of user password patterns is critical since the improvement of new examples may lessen the exertion required by attackers to figure passwords (Yenisey, Ozok and Salvendy 2005).

Notwithstanding numerous worries encompassing their security, text passwords remain the most ordinarily utilized validation strategies. Since complicated text passwords can be difficult to recollect, users will in general pick straightforward passwords. Thus, these passwords are easier to figure. What's more, individuals will in general reuse a similar password crosswise over various accounts so as to limit the quantity of passwords they should recollect. Besides, users will in general use dictionary words as passwords, which would lessen the exertion spent by an attacker to figure them. A decent password contains alphanumeric characters, digits, lowercase and uppercase letters and ought not comprise of words from dictionary. Passwords ought not be recorded in an easily open spot, particularly alongside login area. To counter this, frameworks as a rule expect users to agree to an intricate password approach that may require the user to utilize non-word reference passwords with least length and a specific mix of uppercase letter, special characters (symbols) and numbers (Gaw and Felten, 2006).

It is critical for a User to pick solid passwords that are distinctive for each and every account. A few users utilize same passwords for various accounts. Utilizing same passwords for multiple accounts resembles

utilizing same key to open your home, vehicle and office. On the off chance that the interloper gains admittance to one so he gets the passageway for all. On the off chance that passwords are basic and simple to recollect, at that point they can be effectively cracked. Solid passwords, which incorporate the blend of characters, numbers and alphanumeric characters, are hard to crack however they can't be effectively memorized by the user, which diminishes the ease of use of passwords. While making different records, users regularly set passwords which are noteworthy and subsequently are anything but difficult to figure in this way diminishing the security of their accounts. In 2016, 32 million Twitter accounts and 360 million MySpace account passwords were hacked and their Passwords were leaked (Moscaritolo, 2016).

This examination is a considerable advance forward in understanding the effect of different factors on password made by users. These components incorporate, age, computer science know how, gender, secret word policies and so on. We intend to study user behavior and sentiments with respect to their Passwords.

Understanding Password Management and User Behavior

There gives off an impression of general understanding of what makes a decent password and the significance of good password management. This information nonetheless, does not generally convert into great password management. This could be on the grounds that users are excessively hopeful about numerous parts of the web particularly online security. The predominant user frame of mind seems, by all accounts, to be, "web security is imperative, and security breaches can be cataclysmic, yet it won't transpire." This idealism may clarify why users, professional officials, and even IT experts mismanage their passwords (Schneier 2007).

In view of the genuine results of security slips, organizations allot enormous spending plans to introduce shields to ensure access to their frameworks. The expanded spending has prompted firewalls, authentication frameworks, and different methods being conveyed to keep frameworks secure. Notwithstanding, regardless of these regularly expanding uses and endeavors, there is a variable that no measure of cash can control the user. Concentrating on the user is essential on the grounds that albeit more grounded confirmation methods are accessible, companies keep on utilizing a password-based framework to control framework access. All things considered, even the most advanced security framework ends up futile if users mismanage their passwords. The focal point of this Paper is to inspect the intentions behind password management behavior trusting that this information can improve password security (Furnell, Jusoh and Katsabas 2006).

Users frequently make passwords that are essential which makes them helpless as they are anything but difficult to figure. Numerous investigations have been directed to assess the effect of password creation approaches and password meters on user's password creation behavior. Table 1 outlines couple of such examinations that had been recently conducted (Wash, Emilee, Ruthie and Zac, 2016):

Table 1: General Summary of Understanding Passwords and User Behavior

USER BEHAVIOR	DESCRIPTION
Password Reuse	Reusing same password over numerous sites decline password security. Users re-utilize same password with little adjustment on various accounts. Users offer inclination to password ease of use as opposed to security.
Password Memorability and Security	Users will in general decrease their password security for secret phrase memorability. Difficult Password composition strategy influence users to record or write down their password.
Password Composition Policies	Password arrangement approaches empower users to make solid and secure passwords. Password

	key approach limit users to make secret password under certain criteria and example to make their password secure. Most regularly utilized secret password arrangement is comprehensive8 which compel users to utilize digits, Symbols, uppercase, and lowercase letters.
Password Strength Meter	Password quality and strength meter help during the time spent setting up a solid password through advancement meter. Distinctive password meter have diverse impact on user conduct while making passwords. Visual appearance of password quality meter assumes an indispensable job in setting up a password.

Our investigation supplements these examinations by endeavoring to uncover the most recent patterns in user behavior concerning the choice of their passwords. Additionally, we assess the relationship between users' self-evaluated attention to security and the genuine Strength of passwords. Our discoveries demonstrate that individuals trust themselves to be considerably more proficient of password security than the quality of their passwords really shows (Kong, 2004).

In spite of the extensive writing, the current research does not respond to the two inquiries of most interest to firms:

1. Why do users mismanage passwords? and,
2. What can organizations do to urge users to take part in great password management behavior?

To respond to these inquiries, we investigated the mental intentions behind password management behavior. Our application appeared as a web based electronic survey and an examination that considered password management issues. The inquiries posted on the survey were:

1. Do Users comprehend what comprises a secure password and great password management behavior or is more education required?
2. What are the thought processes behind password determination and password management behaviors? And
3. Are there any distinctions in password management behavior for various types of Accounts?

Our definitive objective in responding to these inquiries is to figure out what firms can do to urge users to adopt great password management practices (Ur, Bees, Segreti, Bauer, Christin and Cranor, 2016).

Survey Design

This section examines the structure and method of reasoning of survey. We structured an online survey that would bring genuine and honest data about passwords from our responders. Responders would regularly take under 5 minutes to finish the study. The survey included statistic data, for example, age, gender and field of study. Socioeconomics of users is illustrated in Table 2 and Table 3 below (Das, Bonneau, Caesar, Borisov and Wang, 2014):

Table 2: Users According to their Age

Age Groups	Number of Users	Percentage of Users
Between 15 to 45	45	89%
46 or Above	8	6%
Other	6	5%

Source: Socioeconomic data collected by self through an online statistical data survey

Table 3: Users According to their Gender

Age Groups	Number of Users	Percentage of Users
Male	57	46%
Female	66	53%
Refused to Disclose	2	1%

Source: Socioeconomic data collected by self through an online statistical data survey

To comprehend the password behavior, we included inquiries, for example, kind of password favored, recurrence of evolving passwords, utilizing forgot password alternative, sharing passwords and so forth. Study additionally included inquiries to test the ease of use, memorability and security inclinations (Proctor, 2002).

In online survey proportion of female respondent was somewhat high than male respondent. 53% were female and 46% were male. The 89% of respondent were 14-45 group of age, 6% were from over 45 groups. 14– 50 group of age respondent were high in rate than over 45 group of age.

Passwords Results

Table 4 below demonstrates the normal account creation time, normal login time and normal number of attempts to login. We found that users took long to review their passwords as they were signing in after 2-3 days for the first time.

Table 4: Password Application and User Login Period for Different Password Policy Types

Types of Policy	Number of Users	Average Time to Create an Account (in seconds)	Average Time to Log in (in seconds)	Average Login Tries
Basic8	26	8	27	1.25
Basic16	25	41	33	1.52
Comp8	30	29	64	2.13
Dict8	40	28	26	1.73

Source: Data collected by self through an online statistical data survey

To determine the user experience and behavior in establishing password creation using the four different policy types (Basic16, Basic8, Comp8, and Dict8) we requested users to fill in the post task questionnaire. The results are summarized in Table 5 below:

Table 5: User Experience while Creating Password

QUESTIONS	BASIC16	BASIC8	COMP8	DICT8
Were password policies helpful for you	Yes 60% No 40%	Yes 67% No 33%	Yes 73% No 27%	Yes 76% No 24%
Are you concerned about your password security?	Yes 76% No 24%	Yes 85% No 15%	Yes 97% No 3%	Yes 92% No 8%
Will you use this policy in future to make your password secure?	Yes 48% No 52%	Yes 67% No 33%	Yes 40% No 60%	Yes 88% no 12%

Are you satisfied with the password you have entered?	Yes 56% No 44%	Yes 86% No 14%	Yes 74% No 26%	Yes 84% No 16%
Did you feel any difficulty while setting your password?	Yes 36% No 64%	Yes 4% No 96%	Yes 77% No 23%	Yes 52% No 48%

Source: Data collected by self through an online statistical data survey

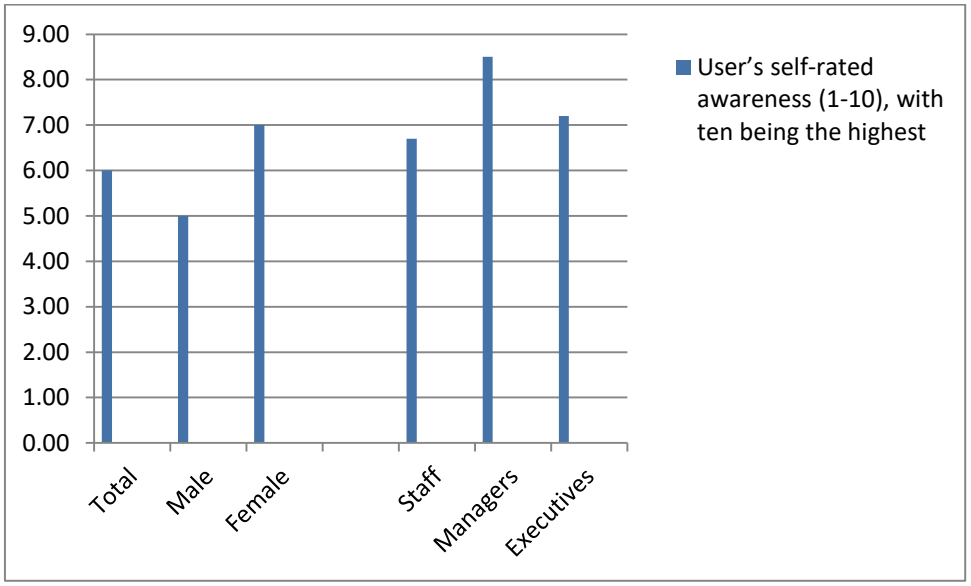
All the password policies were tried and we found that Comphrehensive8 is progressively secure yet less usable. Baisc8 was progressively usable however less secure, 68% of it was effectively cracked. In Basic16, 20% passwords hashes were compromised and in dictionary8, 46% passwords hashes were also compromised, in dictionary8 the hashes which were compromised were the individuals who have dictionary words, however those hashes did not crack that have non-dictionary words. Along these lines, we can conclude that Dictionary8 policy approach is progressively secure and usable than the other three.

Statistical Survey Findings

- Self-Awareness

  So as to get a thought on how users see their insight and of security issues when utilizing internet services, we requested that participants rate their mindfulness on a scale from 1-10 with 1 being entirely unaware of security-related issues and 10 being very aware of security issues (Figure 1 below). Our discoveries show that the normal (self-surveyed) awareness score for all members is 6. Besides, staff and managers with more than 4 years of alliance inside an association rate themselves as more aware than different groups. This moderately high mindfulness rating may be identified with the way that 85% of members trust they have never been compromised. Since the greater part of the members has never been casualties of hacking, they expect that they possess the correct knowledge of password security (CSID, 2012).

Figure 1: Internet user's scale of self-rated awareness (1-10), with 10 being the highest



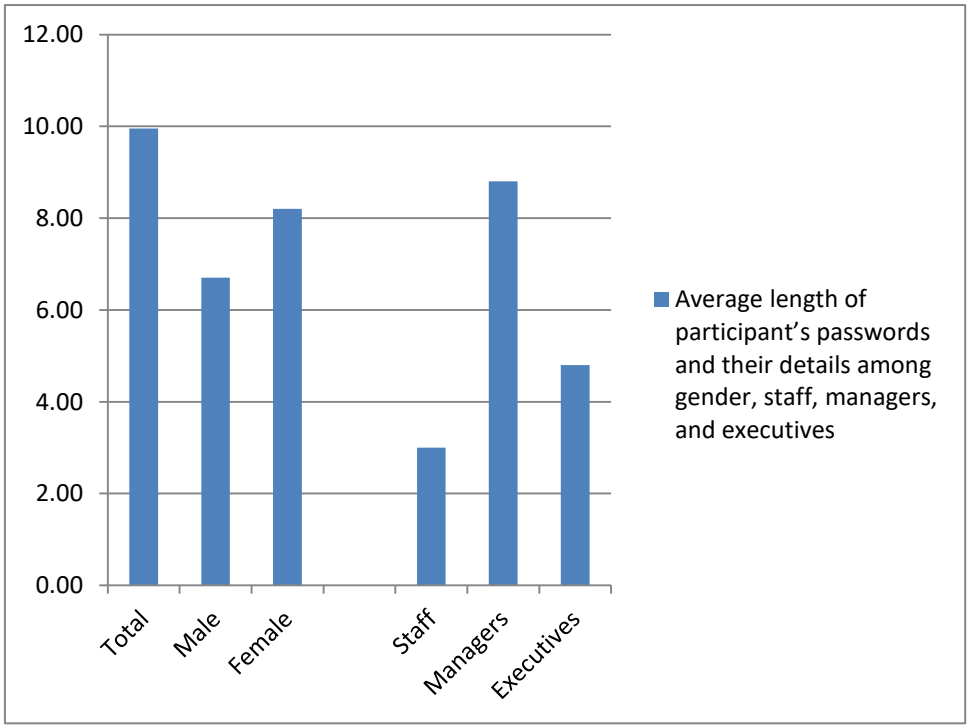
Source: Statistical data collected by self through an online survey

- Password Characteristics

In this survey, we comprised some input with regards to user passwords with a focus on its password length, password presence and position of special characters, passwords containing numbers, and passwords with uppercase letters.

- *Password Length:* Figure 2 below shows that the normal password length for all members is 9.95 characters. Females will in general utilize marginally longer passwords than males and managers will in general utilize longer passwords than employees and executives. Individuals with 3 to 4 years of association inside an organization utilize shorter passwords and lastly, top managers in their areas of expertise utilize longer passwords than that of their staff or employees. We note here that few variables may influence these outcomes. To begin with, organizations support the utilization of complex passwords (despite the fact that it's not actually implemented in their policy). Be that as it may, we found that a few staff member passwords were comprised of less than 8 Characters. Second, new workers appear to be educated about the significance of a long password at the time of initially setting up their passwords (Dell'Amico, Michiardi and Roudier, 2010).

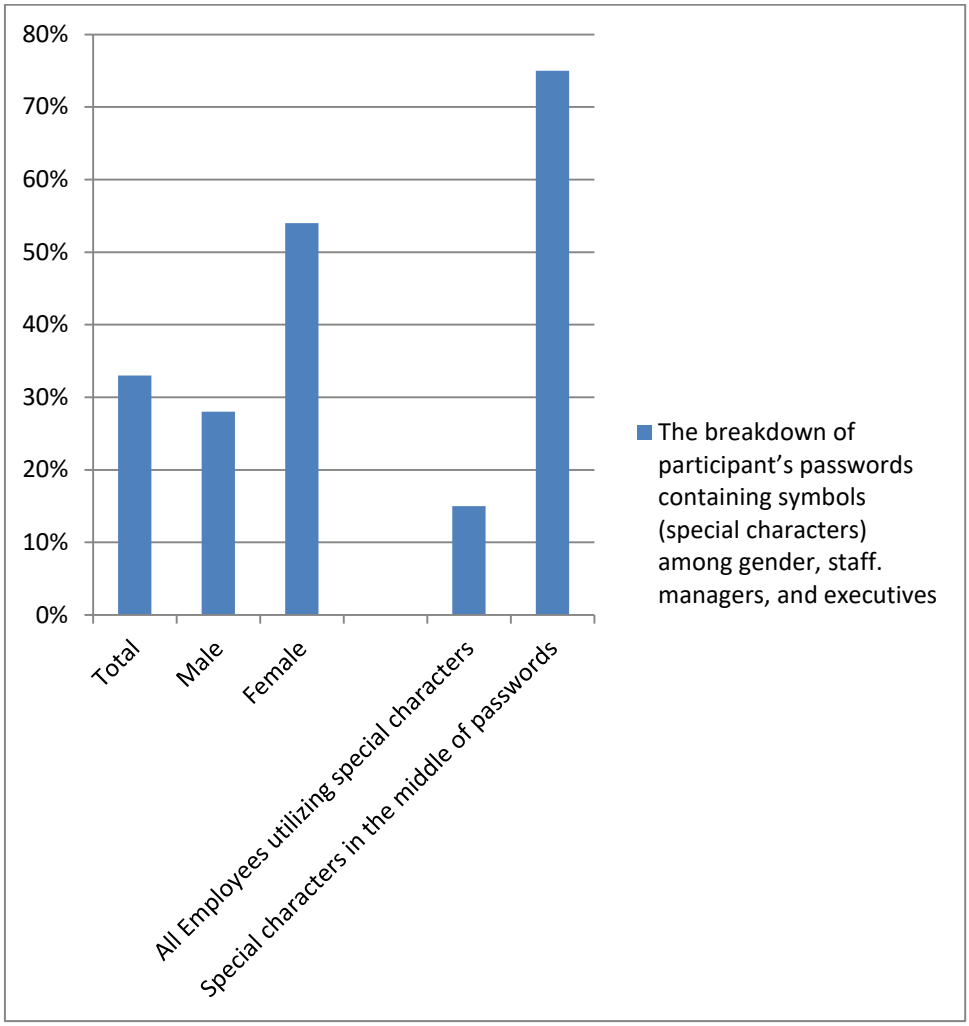
Figure 2: Average length of participant's passwords and their details among gender, staff, managers, and executives



Source: Statistical data collected by self through an online survey

- *Special Characters:* Next we inspect the presence of special characters (symbols) in the user chosen passwords. Figure 3 below demonstrates that approximately 33% of all users utilized a special character. Besides, while the rates are commonly comparable over all groups, just 15% of staff will in general utilize special characters. On the off chance that they utilized a special character, we got some information about its position (area) inside the password. We found that 75% of the respondents place the special character in the middle of their password (in a position other than the first or last characters) (Gehringer, 2002).

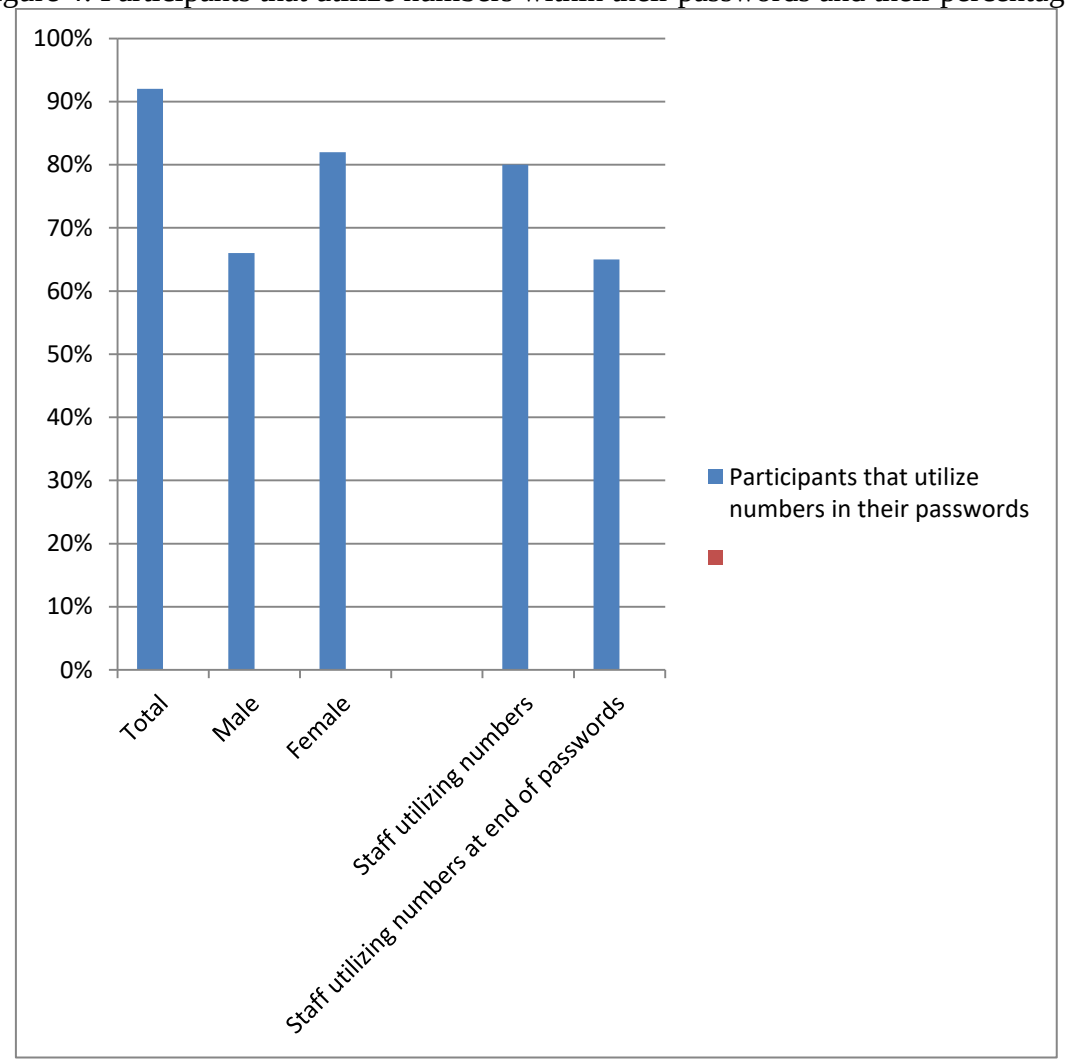
Figure 3: The breakdown of participant's passwords containing symbols (special characters) among gender and those utilizing them in passwords



Source: Statistical data collected by self through an online survey

- *Numbers:* A comparative appraisal was performed for the presence of numbers in user passwords. Per Figure 4 below, simply above 90% of all users use numbers. Comparable rates are found crosswise over groups aside from individuals with more than 4 years of working in an organization where just underneath 80% of them use numbers in their passwords. In addition, nearly 65% of all participants place numbers toward the end of their password (Stanton, Stam, Mastrangelo and Jolton, 2005).

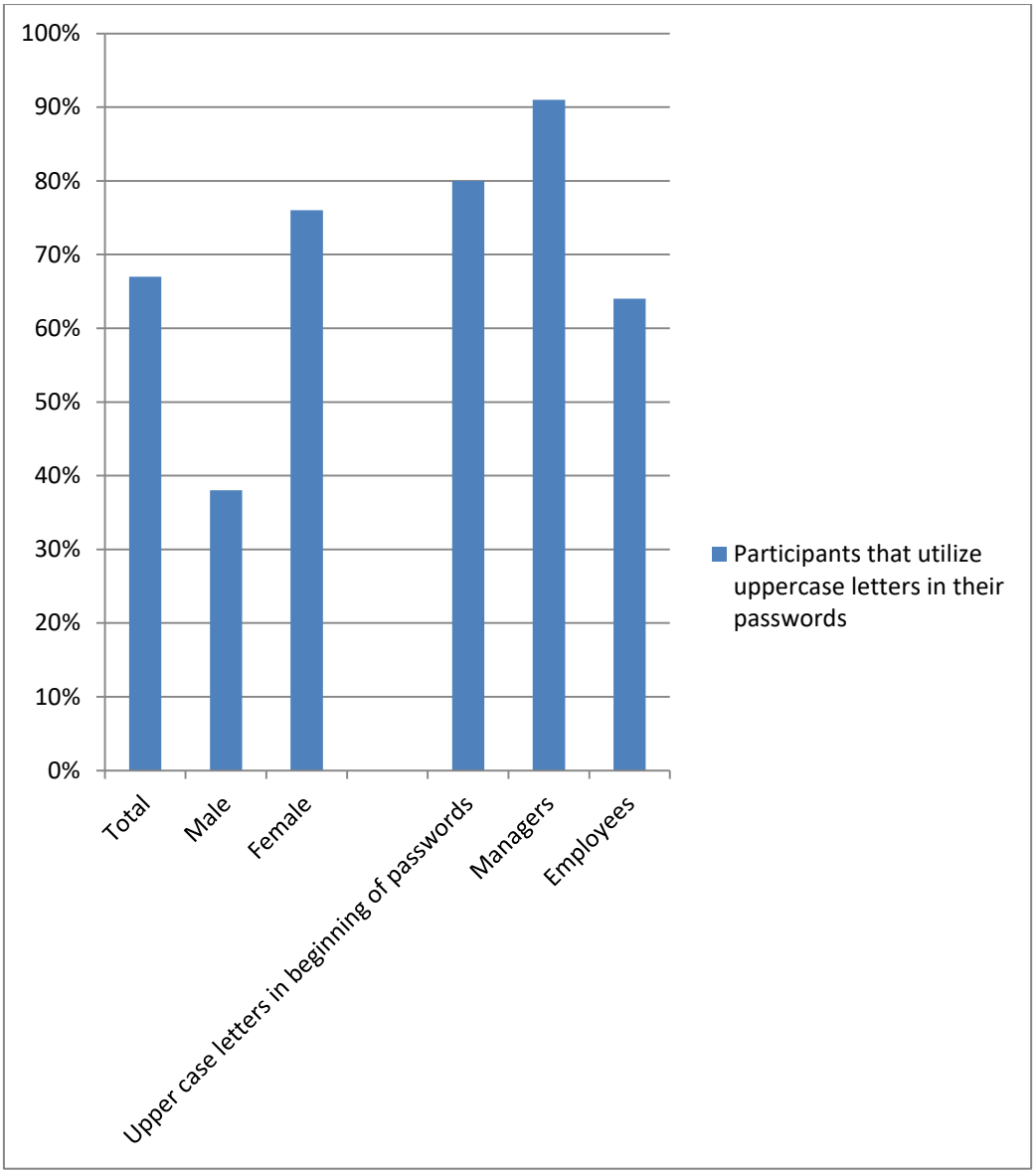
Figure 4: Participants that utilize numbers within their passwords and their percentages.



Source: Statistical data collected by self through an online survey

- *Uppercase Letters:* The findings for uppercase letters are somewhere in between all participants. Figure 5 below indicates that around 67% of those who participated in this survey use uppercase letters. In addition, more than 80% of the users place the uppercase letter at the beginning of their passwords, 91% of which are managers and 64% are employees (Helkala and Bakas, 2013).

Figure 5: Participant's percentage that utilize uppercase letters within their passwords among gender, managers, and employees

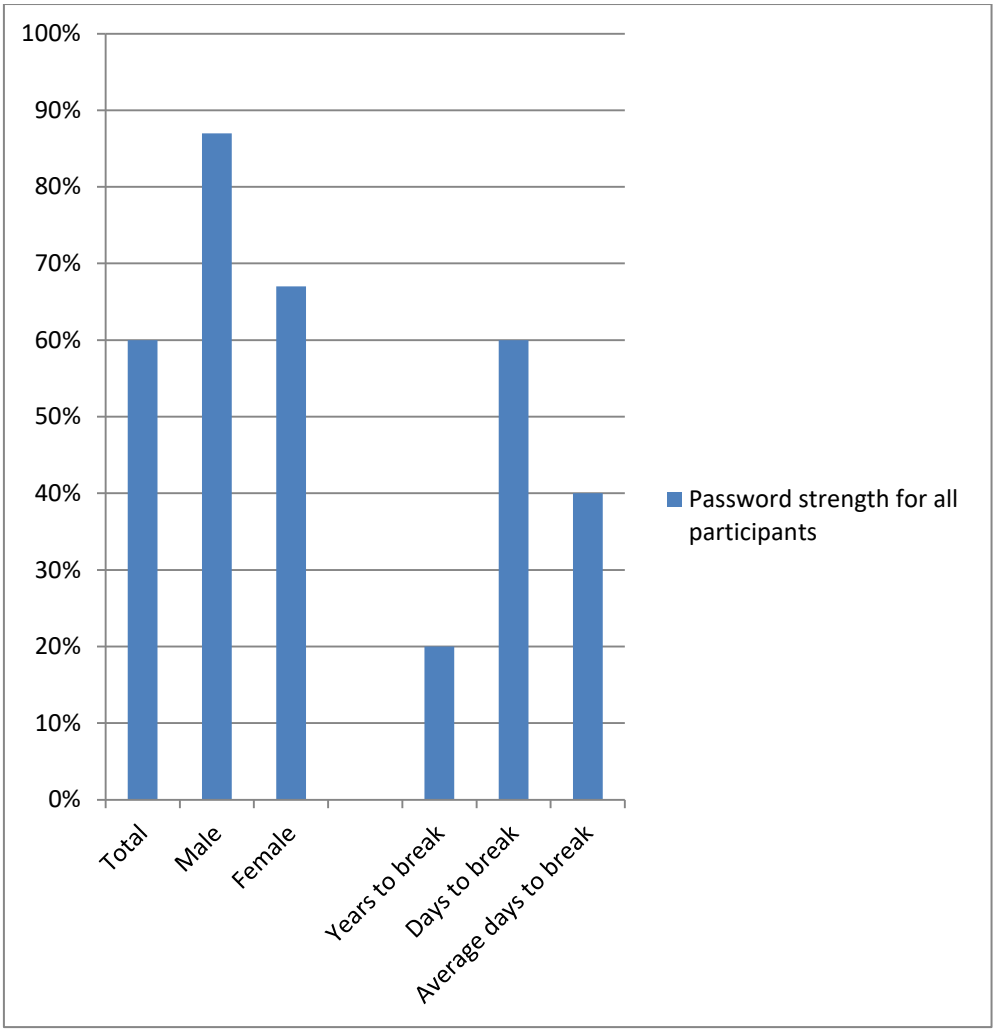


Source: Statistical data collected by self through an online survey

- Password Strength

  Next, we evaluate the quality of the user-selected passwords and relate the outcomes to the awareness level that users revealed. Figure 6 below demonstrates the level of users whose passwords will take fewer days or years to break and the average days to break them. Most of passwords (60%) can be cracked inside days. Not very many passwords would expect years to break, averaging 20%. Around 20% of passwords crosswise over assignments expect a very long time to break. Be that as it may, staff individuals appear to have the weakest passwords. Most of members in every office have passwords that are breakable inside days as well (Kaspersky, 2016).

Figure 6: The strength of participant's passwords including a breakdown according to gender and time to crack

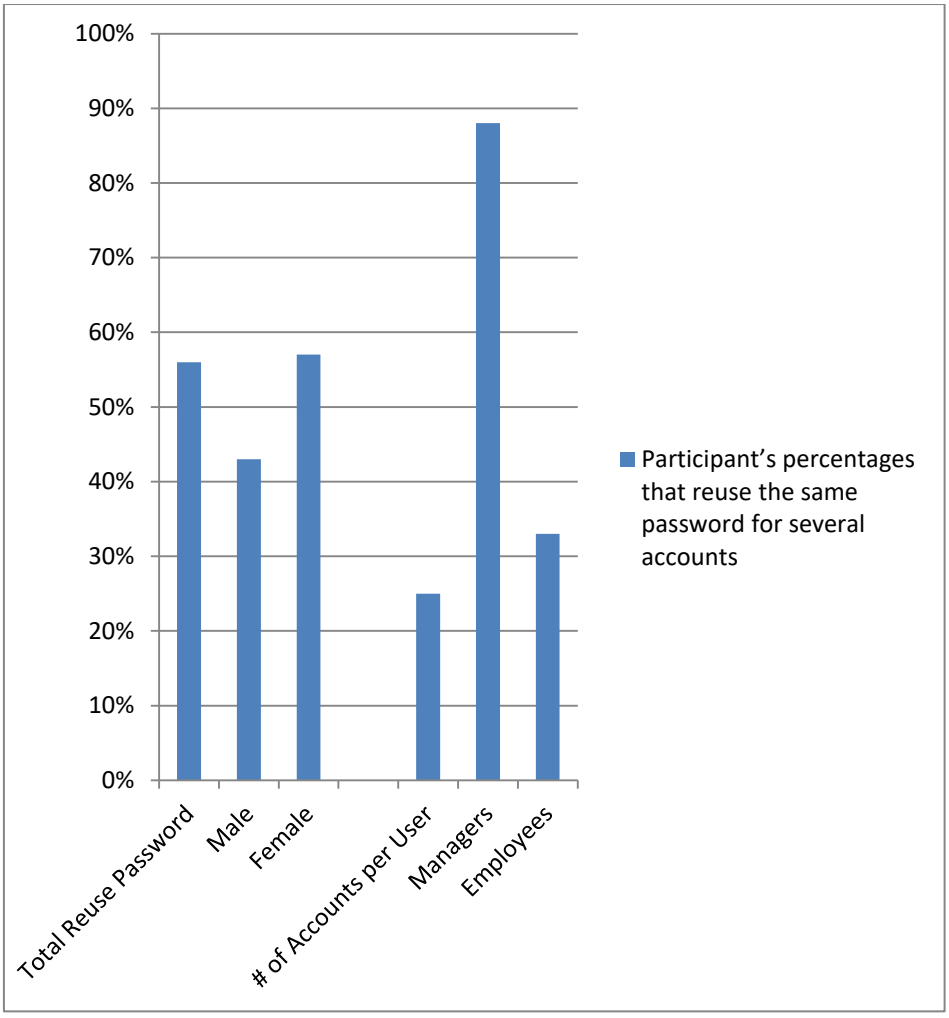


Source: Statistical data collected through an online survey

- Password Reuse

  Reusing passwords over different accounts can duplicate the effect of password cracking. In this manner, we next evaluate the normal number of records for which our members utilize the same password. As found in Figure 7 below, simply over portion of the members utilize similar passwords for multiple accounts. In addition, employees will in general reuse their passwords the most much of the time though individuals with more than four years of connection with an association will in general reuse the passwords the least regularly (around 33% of them reuse passwords). Shockingly, this propensity is far reaching since it is evaluated that the typical internet user has 25 online accounts that require passwords (Florencio and Herley, 2007).

Figure 7: Participant's percentages that reuse the same password for several accounts



Source: Statistical data collected by self through an online survey

- Strengthening the Password

  So as to feature the significance of special characters in expanding the password complexity, we requested that all participants embed a question mark '?' in the second position and reconsidered the quality and strength of the new passwords. We chose to pick the second position since some dictionary attacks may probably take out special characters in the first and last positions.

  Figure 8 below shows that including a question mark at the second position obviously improves password strength fundamentally. For instance, around 55% of passwords presently require years or hundreds of years to crack contrasted with just about 25% without the '?' symbol. Note that while including any character in the second position builds the password quality and strength, a special character may be to recall and will result in a password that doubtlessly won't exist in a dictionary (Shay, Kelley, Leon, Mazurek, Christin and Cranor, 2010).

Figure 8: Participant's password strength after adding a question mark (?) after the first position in their passwords including the length (time) it takes to crack.

Source: Statistical data collected through an online survey

Conclusion

In this study, we examined the user behavior concerning password selection and determination. We surveyed the strength of user-selected passwords and registered the connection between the quality of these passwords and self-evaluated awareness of security concepts. We found that most of user passwords could be undermined. Note that the tradeoff span gauge is a liberal one dependent on an attacker with access to a normal computer. Besides, a minority of users utilize special characters or symbols. These special characters

will in general be put some place in the middle of the Password (neither toward the start of the Password nor toward the end). Numbers and uppercase letters are significantly more generally utilized. In any case, uppercase letters are regularly utilized toward the start of the passwords and numbers are normally put toward the finish of the Password, making it simpler for attackers to make progressively powerful dictionaries with properties that line up with these propensities.

Furthermore, we explored the ease of use of password policies and users' impression of password security. We reasoned that numerous users favor same passwords for multiple accounts to decrease the weight of recollecting multiple passwords. Such users disregard the risk that every one of their records can be undermined. Likewise, convenience is regularly favored over security and complex password strategies irritates user.

We likewise saw that when users are compelled to utilize complex passwords, they will in general reuse same password on various accounts to improve the memorability of generally complex password. Majority share of users use relative names, individual data, and dictionary words in their passwords. Such users don't know about the defenselessness of these passwords. Youthful users are progressively worried about the security of their accounts, and in this manner, they want to make complex passwords. Password meters are likewise useful in making users select solid and unique complex passwords. In any case, content based passwords remains an aggravation for ordinary users and complex password prerequisites makes it increasingly hard to recall and remember passwords.

Recommendations

In view of the consequences of this examination, we propose the following three recommendations:

- The first proposal is to authorize and enforce a more astute and increasingly complex password policy. For instance, the arrangement ought to require a base length Password with a mix of uppercase, lowercase, numbers and special characters (symbols). Be that as it may, uppercase letters ought to be put in different areas of the password, and not just simply in the beginning or the end of a password. Numbers ought to likewise be put some place in the middle of the passwords. Additionally, it would be extremely useful if the framework played out a programmed check and contrasted the proposed password with regular dictionaries before endorsing and approving it.
- The second suggestion is uphold an intermittent or periodic password change. Besides, the National Institute of Standards and Technology (NIST) recorded a few electronic verification guidelines, which increment the password guessing probabilities making it harder to crack (Burr, Dodson and Polk, 2006).
- The third and final recommendation is to propose and properly educate users about PC security and the significance of a solid and strong password. The properties of a strong Password were illustrated with survey participants, who were then educated on how to refresh their passwords appropriately and on the most proficient method to compose a noteworthy yet complex password. Be that as it may, given the high stakes and across the board security breaches, an appropriate and ceaseless education of the significance of choosing complex passwords stays an essential part to eliminate cracks or account breaching, and insure safety and security of their multiple online accounts with passwords that are complex and unique to each account.

References

1. Burr, W.E., Dodson, D.F. and Polk, W.T., 2006. Electronic authentication guideline. *National Institute of Standards and Technology* [Online] Available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-3ver1.0.2.pdf [Accessed: 21 February 2019].
2. Cranor, L. F., Hong, J., Reiter, M. K. 2016. *Supporting Password-Security Decisions with Data*. PhD Thesis, Carnegie Mellon University
3. CSID, 2012. *Consumer survey: Password habits a study of password habits among American consumers.* Austin, Texas, U.S.A.: Office for White Papers Operated by Exeprian
4. Das, A., Bonneau, J., Caesar, M., Borisov, N., and Wang, X., 2014. The Tangled Web of Password Reuse. *Joseph Bonneau* [Online] Available at: http://www.jbonneau.com/doc/DBCBW14-NDSS-tangled_web.pdf [Accessed: 23 February 2019].
5. Dell'Amico, M., Michiardi, P., and Roudier, Y. 2010. Password strength: An empirical analysis. *Proceedings of the IEEE INFOCOM,* San Diego, 14-19 March, 2010. CA, USA, pp. 983-991.
6. Florencio, D. and Herley, C. 2007. A large-scale study of web password habits. *Proceedings of the 16th International Conference on the World Wide Web*, Banff, 08-12 May, 2007. Alberta, Canada, pp. 657-666.
7. Furnell, S., Jusoh, A., and Katsabas, D. 2006. The challenges of understanding and using security: a survey of end-users. *Computers & Security* [Online] 25. Available at: https://www.researchgate.net/publication/223844978_The_challenges_of_understanding_and_using_security_A_survey_of_end-users [Accessed: 29 February 2019].
8. Gaw, S. and Felten, E.W. 2006. Password management strategies for online accounts. *Proceedings of the 2nd Symposium on Usable Privacy and Security*. Pittsburgh, 12-14 July, 2006. Pennsylvania, USA, pp. 44-55.
9. Gehringer, E. 2002. Choosing passwords: security and human factors. *International Symposium on Technology and Society* 11(9), pp. 369-373.
10. Helkala, K.M., and Bakas, T.H. 2013. National password security survey: Results. *Proceedings of the European Information Security Multi-Conference.* University of Plymouth Press, 8-10 May, 2013. Lisbon, Portugal, pp. 23-33.
11. Kaspersky. 2016. *Kaspersky lab's secure password check* [Online]. Available at: https://password.kaspersky.com/ [Accessed: 3 March 2019]
12. Kong, H. 2004. *Password Memorability and Security : Empirical Results* [Online]. Available at: https://prof-jeffyan.github.io/jyan_ieee_pwd.pdf [Accessed: 3 March 2019].
13. Moscaritolo, A. 2016. *Hacker selling 32M twitter accounts on dark web*. PC Magazine [Online]. Available at: http://www.pcmag.com/news/345121/hacker-selling-32m-twitter-accounts-on-dark-web
14. Proctor, R. W. 2002. Improving Computer Security for Authentication of Users: Influence of Proactive Password Restrictions. *Behavior Research Methods, Instruments, & Computers* 34(2), pp. 163-169.
15. Schneier, B. 2007. *The Psychology of Security* [Online]. Available at: http://www.schneier.com/essay-155.html [Accessed 4 March 2019].
16. Shay, R., Kelley, P. G., Leon, P. G., Mazurek, M. L., Christin, N., and Cranor, L. F. 2010. Encountering Stronger Password Requirements : User Attitudes and Behaviors Categories and Subject Descriptors. *Cylab Usable Privacy and Security Laboratory* [Online]. Available at: https://cups.cs.cmu.edu/soups/2010/proceedings/a2_shay.pdf [Accessed 5 March 2019].
17. Shen, C. 2016. User practice in password security: An empirical study of real-life passwords in the

wild. *Computer Security* 61, pp. 130-141.

18. Stanton, J., Stam, K., Mastrangelo, P., and Jolton, J. 2005. Analysis of end user security behaviors. *Computers & Security*, 24, pp. 124-133.
19. Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N., and Cranor, L. F. 2016. *Do Users' Perceptions of Password Security Match Reality?* [Online] Available at: https://www.blaseur.com/papers/chi16-pwperceptions.pdf [Accessed 5 March 2019].
20. Wash, R., Emilee, R., Ruthie, B., & Zac, W. 2016. Understanding password choices: How frequently entered passwords are re-used across websites. *Proceedings of Symposium on Usable Privacy and Security (SOUPS).* Denver, 22-24 June, 2016. Colorado, U.S.A., pp. 1-15.
21. Yenisey, M., Ozok, A., and Salvendy, G. 2005. Perceived security determinants in e-commerce among Turkish university students. *Behaviour & Information Technology Journal* 24(4), pp. 259-274.