Scientific and Practical Cyber Security Journal (SPCSJ) 4(2): 45-58 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

OUR PASSWORD SECURITY PRACTICES: SECURE OR VULNERABLE

Safwana Haque BRAC University, Dhaka, Bangladesh
Farhana Haque Anwer Khan Modern University
Md Abdul Haque International University of Business Agriculture and Technology

ABSTRACT: Text-based password is the most commonly used method to authenticate systems, and plays a vital role in keeping our data safe from attackers, therefore, it is important to have adequate knowledge for secured password practices. This study carried out an online survey of 500 people to study their response to password security. It was seen that 63% of the participants were vulnerable to password attacks because of their chosen methods. People of age 65 and above were found to be at the highest risk, while 80% of the female population have either never experienced or do not have any idea of a breach in their account. It was seen that 90% of the participants used information of personal significance in their lives, but 53% would still like secure passwords. This study suggests improvements for each chosen method that would make our system more reliable and immune to attacks.

KEYWORDS*: Password Security, Security Awareness, User Behavior, Security Practices, Cybersecurity*

INTRODUCTION

Cisco defines cyber-security as 'the practice of protecting systems, networks, and programs from digital attacks'(CISCO n.d.). The users, programs and methods must all have an individual contribution to be safe and secure in a network. The users of the network or system must understand what is required to keep it safe such as choosing a secure password, accessing e-mails and websites that are safe, backing up data occasionally, etc (Armerding 2018). There are many ways of keeping a network, computer or account safe and password security is only one vital part of a more complex problem of providing security in an organization.

Passwords are the most popular and commonly used methods to restrict access to unauthorized users of a system or account (Techopedia n.d.). A password is usually a combination of alphabetic, symbolic, alphanumeric, or numeric characters. As mentioned, passwords are meant to restrict access to unauthorized users. It has been seen previously that the user passwords of very famous companies such as Yahoo, eBay, Uber, etc. have been hacked by using some sophisticated algorithm, and confidential information like date of birth, email address and password were stolen. As of 2013, Yahoo reported a huge security breach where three billion of its user accounts were compromised and this led to a loss of $350 million in sales (Armerding 2018). The massive loss and alarming numbers of stolen information lead to a huge concern on password security.

Text-based passwords are the most commonly used authentication methods and monitoring the patterns of passwords of users regularly is necessary to understand the vulnerabilities that exist in a network. In this way, users could be educated and stronger securities policies and techniques could be implemented to keep data safe from attackers.

RELATED STUDY

Password security should be taken seriously by individuals and organizations where people should properly know how to create good passwords, change it occasionally and also record it safely and

properly for later use (Techopedia n.d.). An issue of choosing passwords is that people tend to choose very easy passwords, most of all they tend to choose from one set of characters e.g. all small letter alphabets which would possibly be a word from the dictionary or a name of someone. Another issue of password security is when the actions of ex-workers who would have very detailed knowledge of the system and resources in an organization cannot be controlled(Morris and Thompson 1979). In these cases, passwords become very vulnerable to attacks. Password security should also be made as convenient as possible for users, so that unauthorized people may not be able to log in and also users that are logged in will not be able to carry out any unauthorized or illegal activity (Morris and Thompson 1979).

(Morris and Thompson 1979) conducted an experiment on the choice of passwords created by users when they were not enforced with any criteria of password creation. A total number of 3,289 passwords were collected out of which 477 were four alphanumeric characters, 706 were composed of five letters where all the letters were either in upper-case or lower case characters , and 605 were six-letter passwords, all in lower case. The authors further ran a test to see how fast they could identify the passwords with a matching algorithm and if the passwords were from the dictionary. It was reported that one-third of the passwords were words from the dictionary and took five minutes to run the test. This experiment was carried out in 1979 on a UNIX system and it is expected that with the advancement of hardware and software technology now, lesser time would be required identify these passwords (Klein 1992). It was suggested that users should be forced to use longer passwords, select passwords from a large character set or use a program that would generate the password for the user. In 1989, a survey carried out by (Klein 1992) on password showed that out of 15000 participants, 2.7% used their usernames as their passwords and this was easily cracked in the first 15 minutes of the experiment.

Some suggested ways of formulating a good password are the use of room, social security, license plate or telephone numbers, names of streets, cities or first names with the first letter in uppercase, and also words from the dictionary that are spelt backwards (Morris and Thompson 1979). Although it was suggested in (Klein 1992) that passwords that contain these numbers solely is not a good security practice because hackers understand that people will choose numbers that have special meanings attached to it. These should be combined with other words or numbers that make it difficult to guess. Using words from the dictionary are known to be bad practices as this could be easily cracked and also common words spelt backward as mentioned in (Morris and Thompson 1979) are not advisable to use as passwords (Klein 1992). However, using a combination of words is a good practice, and if combined with a punctuation mark or uppercase characters increases its difficulty of being cracked. Using the initials from a long sentence also makes it difficult (Klein 1992). Another way of checking the vulnerability of a password is by using a password checker that would immediately reject common words from the dictionary, initials from the user's names, usernames as passwords, patterns of keys from the keyboard, words shorter than specific length, etc.

Apart from the fact that users select very easy passwords that could be hacked easily, other ways of identifying passwords are by gaining access to the system, eavesdropping on the communication line between the user and the system and studying the way the password matching algorithm works (Lamport 1981).

These were experiments or studies carried out in the 20th century, but what about the 21st century? Have the password choosing habits of people changed? Are people well aware now as the technology is improving?

A survey carried out by (Riley 2006) on the knowledge of user password security showed that out of 315 respondents, 73% knew that it was advisable to change passwords every 6 to 12 months, but 53% reported not changing passwords till it was necessary. 51% understood that using special characters is a good practice but only 4.8% used such characters in their passwords. 71% reported that using words of interest to a person or strong meaningful words should be avoided as this could easily be hacked if a profile study was conducted by the hacker, however 50% reported using these words. Just like

meaningful words, 68.3% understood that personal numbers such as telephone, date of birth, etc. should be avoided but 55% reported that they used such numbers in their passwords. 60% of the respondents reported that they do not change their password even if it depends on the complexity of the situation such as bank account passwords and all these are based on the fact that users have a difficulty remembering too many passwords. These studies show that users are actually aware of the security issues, but always go back on using simple strategies to remembering passwords which makes it vulnerable to attacks.

(Gaw and Felten 2006) carried out a survey with 49 undergraduate students and it showed that the respondents understood that password security was essential but had difficulty remembering passwords. Some responded that they had variations of a particular password which they used for different websites, and this had helped them remember passwords. They understood the necessity of using randomly generated password, but they still pictured an attacker as a human, hence they chose passwords difficult for a human to crack, but failed to realise that sophisticated algorithms are now used to hack into accounts. Some also mentioned that they would change their passwords regularly if they were asked to do so, and it was suggested that websites should keep a record of the frequency of logins from users. The websites should then send reminders to the users to change their passwords from time to time. It was observed that the users are educated, have technical knowledge, and easily adapt to new and emerging technologies, but they still have difficulty understanding the method of attacks.

(Florencio and Herley 2007) conducted a three-month study on password habits of half a million users and it was found out that an average user had approximately seven passwords where each password was reused in approximately four other websites. During a three-week period, it was also observed that about 436, 000 clients visited a phishing site, so on an average about 0.4% of the population visits a malicious website annually. It was found that people tend to forget their passwords a lot and at least 1.5% of Yahoo users forget their password each month and this could be because a user has 25 other accounts and signs in into at least 8 per day. This has already been reflected in the study carried out in (Gaw and Felten 2006) where it was mentioned that with time, remembering passwords would be tougher as people will have more accounts to handle.

Over time, some websites or management systems came up with password creation policy and this meant that a password must have a minimum of 6 to 8 characters, contain an uppercase and digit, and it must not be constructed from dictionary words. This policy was introduced in a university and(Shay et al. 2010) carried out a survey on user feedback few days after the policy was introduced. The survey included 470 respondents from the university; it was found out that the change in password policy annoyed most users even though they understood that their accounts were trying to be better protected. Users who created and forgot their passwords were more annoyed and were likely to write their passwords down in a place that would be fast to access, but would be less secure. The study, however, showed that forgetting password did not depend on IT literacy or age factors. In fact, women tend to forget their passwords more than men. One-fourth of the users had shared their old and new passwords with someone. The results obtained showed that younger generation mostly shared their passwords with someone. Three-fourth of the participants reused passwords and half modified old passwords which indicates that even when forced to change passwords, many do not create completely new passwords which still is a breach to password security as obtaining access to any one account of a user can enable access to other accounts. About 69% of the female participants reported using slight modifications of old or other passwords used for other accounts compared to 55% of the male respondents. More than 80% of the users still used a dictionary word and attaching special characters to it which indicates that people still like using words they can easily remember or have special meaning to them.

As mentioned in (Shay et al. 2010) text-based passwords are still very popular as it does not require any hardware device, and is cheaper to implement than other methods such as the biometric authentication procedure. This method is however, vulnerable to dictionary attacks as people tend to use words that are used on daily basis, and also shoulder surfing which is also known as spying. This means the attacker simply spies and observes the user entering the password (Raza et al. 2012). It is easy to pick up the

password if the user is typing slowly, hence when creating complex password policies, this should be considered.

In a survey carried out by (Awad et al. 2017) on 140 university students, it was found that females were more inclined to use longer passwords than males. Less than one-third of the participants used special characters and they were used mostly in the middle of the passwords; 90% used numbers, which were used at the end of passwords making them weak as the words could easily be guessed. On the average, 48.5% use uppercase but 80% of these have it as the first letter making it easy for attack, as spellings or sentences mostly start with capitals and a combination of characters could easily guess the password. 60% of the passwords used in the university could be cracked within days. The study clearly showed that people tend to think they are secure, but their password habits prove it otherwise.

It is necessary to educate users on their password choosing strategies, strengths and weaknesses to improve cyber security; hence a tool was devised in a study which would allow users to enter potential passwords and the tool would predict how strong or weak the chosen password was. As seen in (Tsokkis and Stavrou 2018), only 10% of 30 respondents used random passwords, while there was a high tendency of using dates as part of passwords (40%). 47% of the users entered predictable passwords and after the test, 80% of the users agreed to change their password understanding the lack of security of their passwords. It was emphasized by researchers that users should be educated more frequently on their password habits and policies should be enforced so that users are obliged to choose strong passwords.

Computers and the internet were introduced long time ago in most of the places discussed above, but as for Bangladesh, internet was introduced in 1995 and in 1996, there were only two internet service providers in the whole country (Hamidur 2009). In February 2019, it was reported that there were about 92 million internet users (Anonymous 2019). It is therefore necessary to continuously monitor user password trends as the country is progressing very fast towards internet usage. As it can be seen, humans play a key role in maintaining a secure system, as their decisions can have either a positive or negative effect on the security of accounts and a network as a whole. The objective of this study was therefore to understand the password choosing strategies, effects of poor password practices for accounts and suggest necessary steps to rectify these problems.

METHODOLOGY

This study was carried out in Bangladesh in 2019, using an e-survey comprising of 28 questions, of which five collected the demographic information of the respondents, while the rest were used to determine the behavior of the respondents towards password practices. A total of 500 Bangladeshi respondents participated in this survey and the results of the survey were broadly categorized according to the following demographic parameters:

- **Gender**: respondents were classified into male and female gender groups. About 65.9% of the respondents were male, while 34.1% were female.
- A**ge**: respondents were grouped into five categories; 18-24 (56.2%), 25-34 (33%), 35-49 (7.8%), 50-64 (2.2%) and >=65 (0.8%). It was noticed that the younger the age group, the more the number of respondents. This could be attributed to the possibility that younger generations are more tech-savvy whereas the older generations are not.
- **Technical know-how**: respondents were categorized into four groups depending on their educational and technical backgrounds, that is, science background (54.2%), non-science background (16.8%), IT professional (15%) and non-IT professional (14%).

The survey conducted comprised of different types of questions but most were of dichotomous and multiple-choice types. About five questions were open-ended which were used to understand the users' ability to discern between weak and strong passwords. Detailed analysis and explanation of the results obtained from the survey conducted are given in the following section.

RESULTS AND DISCUSSIONS

NUMBER OF PASSWORDS

Online dependency is immense nowadays as most websites require users to have an account with them in order to carry out some form of transaction or communication with them. There are many different types of online accounts possible such as email clients, bank accounts, health services, e-commerce sites, utility services, social media accounts, and government services. ***Fig. 1***. shows that people most commonly have at least five different types of online accounts. From the total number of respondents, it was found that almost 70% of people have at least 5 or more different account types which could mean that one could own up to 10 or more accounts. For example, someone could have Yahoo, Gmail and Hotmail email client accounts at the same time and also could use Twitter, Facebook, Instagram, Viber, WhatsApp, and Skype social media applications. In this way, one could have a large number of online accounts.

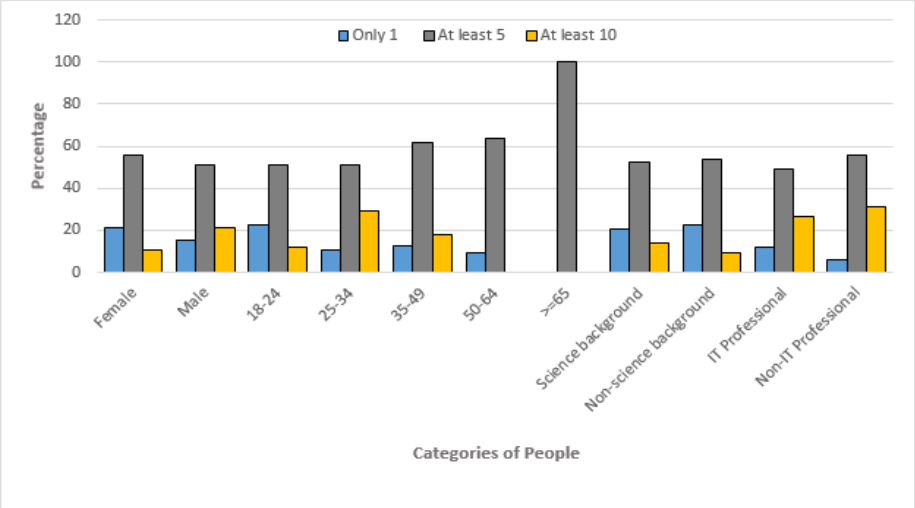

Fig. 1. *Number of online accounts owned by different categories of people*

PASSWORD COMPOSITION

Most online accounts nowadays set some password requirements such as length of passwords, combination of characters, numbers and cases. To satisfy these requirements, users use different pieces of information to form a password combination. From *Error! Reference source not found.*, it can be seen that 90% of the users used the most common types of personal information such as names of self, relatives, pets etc.; a number such as telephone number, identification number etc.; a date or year of relevance such as birthdays, anniversaries etc.; something about oneself such as hobbies, likes and dislikes etc.; a dictionary word found in a language or a combination of some or all the above mentioned. Use of commonly known facts about oneself is highly dissuaded as these pieces of information can be easily gathered from online stalking or profiling.

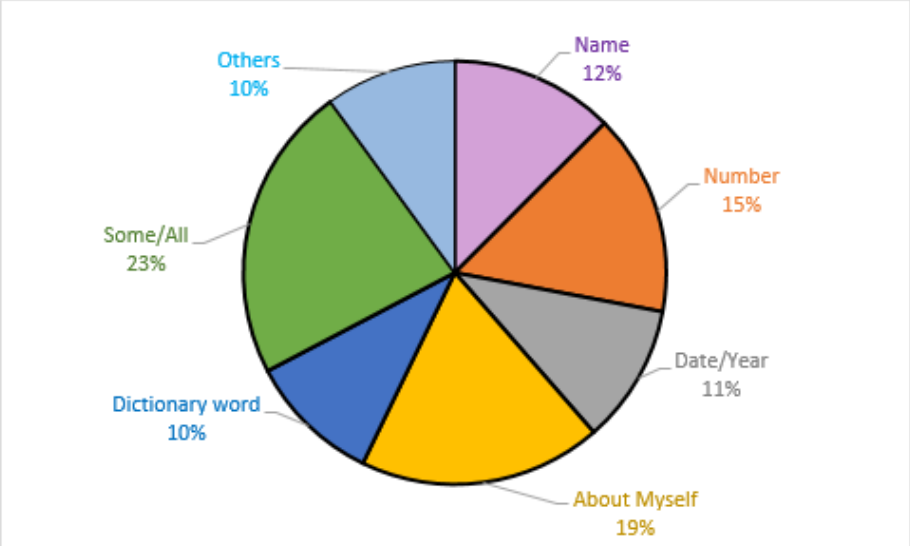

Fig. 2. *Most-used pieces of information to form passwords*

PASSWORD REMEMBERING TECHNIQUE

As the number of online accounts owned per person increases, the more challenging it becomes remembering and maintaining different passwords for each account. There are several ways employed by people which help them in remembering their passwords as shown in ***Fig. 3***.

It can be seen that most popular choices for recalling passwords are choosing an easy password and writing down in a book, notepad, diary, etc. for later reference. Choosing easier passwords is higher amongst the female participants (38%) compared to the male participants (27%). Usage of easy passwords is a very common practice amongst all categories, and writing down passwords is seen to be very widely used in the age group of 50-64 (45%). Both these methods are not recommended as easy passwords can be easily cracked or guessed by others and a book of passwords can be dangerous if it falls in the wrong hands as it would contain all the usernames and passwords of all accounts the owner has. Using passphrases unique to each account may be a better choice, for example, having Y! I5 my 1st 3m@il @ccT for a Yahoo account and 1 @m v3rY !rr39u1@r on F8 for a Facebook account.

Another option would be using a password manager. A password manager is simply a software which could be used to store passwords in an encrypted format, and the user would require a key password to view or manage the passwords stored. However, one must be careful and smart about selecting the master key that would keep all other passwords safe.

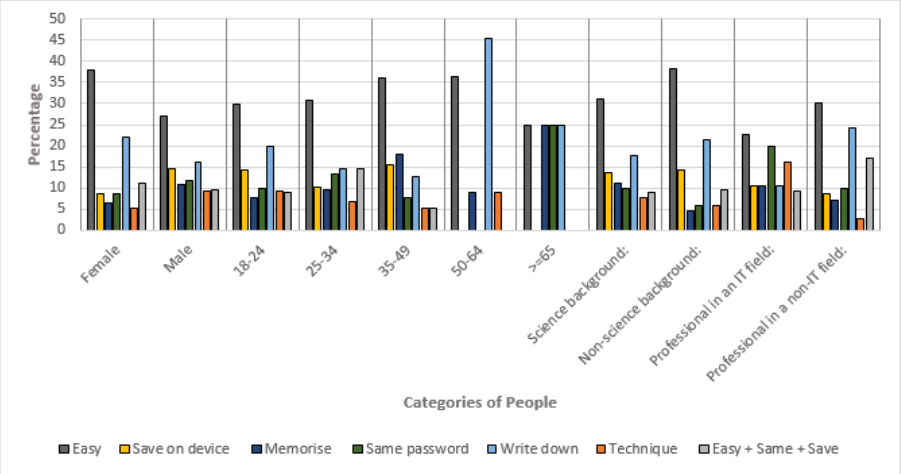

Fig. 3. *Remembering techniques among the different categories of people*

PASSWORD RE-USE

It is recommended to use a different password for every different account so as to prevent access to all of one's accounts in case a third-party gains access to one password/account. From this study, it was seen that 32% of all respondents re-use their passwords in some/all of their accounts. From ***Fig. 4***, it can be seen that people who are 65 years and above are more than likely to re-use their passwords. It is also surprising to note that those from an IT background have a high percentage (40%) of password re-use.

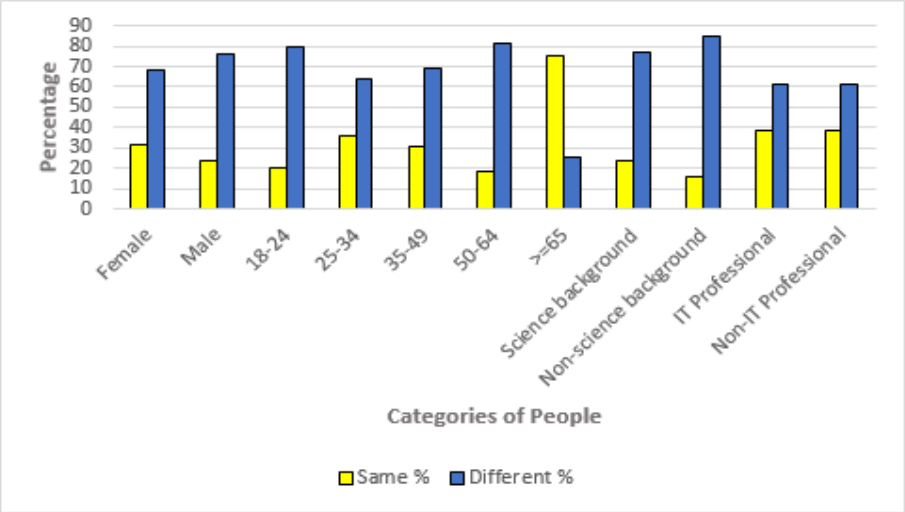

Fig. 4*. Password re-use among the different population categories*

PASSWORD CONFIDENTIALITY

Passwords are meant to be personal and private at all times to the authorized parties only to avoid breach of confidentiality such as the unauthorized access and use of data. However, it was seen from the survey that users gave out their passwords deliberately to different people without thinking about or realizing the repercussions of doing so. ***Fig. 5*** indicates that only 43% of the respondents did not share their passwords, while up to 6% of the respondents shared their passwords with at least five people or even

more. ***Fig. 6*** presents the percentages of whom people mostly shared their passwords with. Even though 87% of the respondents shared their passwords with their loved ones (husband, wife, boyfriend, girlfriend, siblings or friends), who can mostly be assumed to be trustworthy, sharing passwords can still be very risky as these people may intentionally or inadvertently compromise sensitive data or account details.

Fig. 7 shows that at least 50% of each of the respondents across all of the demographic parameters compared have shared their passwords. It can also be seen that among all the different groups of respondents, the people above the age of 65 years can be the most vulnerable as 80% of this group share their passwords. Alarmingly, it was found from the survey that only less than 1% of the respondents who shared their passwords with some other person(s) changed their passwords afterwards.

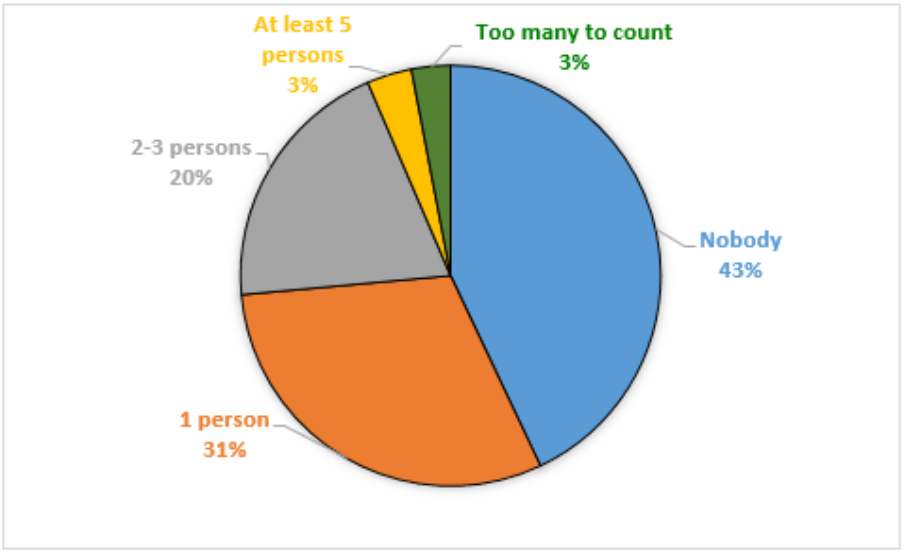

Fig. 5. *Number of people passwords was shared with*

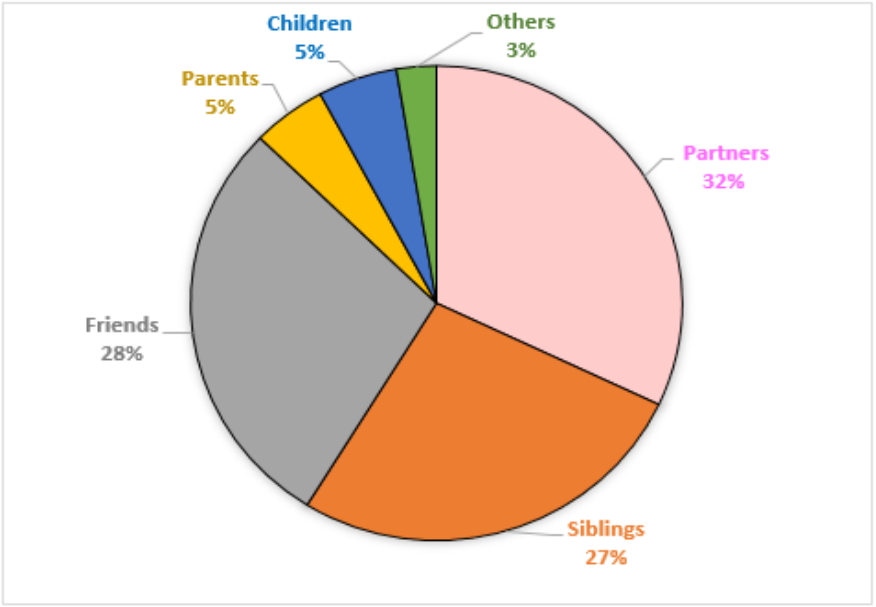

Fig. 6*. Categories of people passwords are shared with*

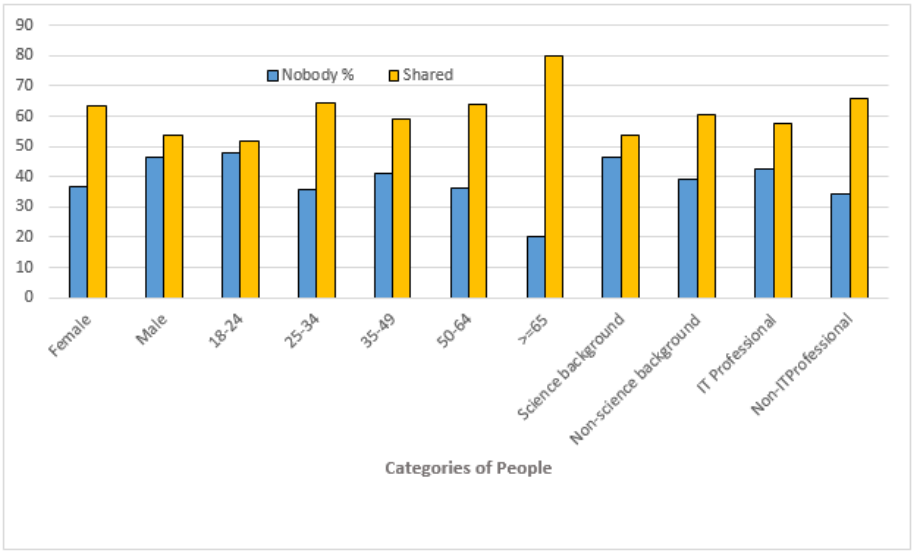

***Fig. 7**. Password sharing percentages among the various demographics compared*

PASSWORD CHANGE FREQUENCY

Various experts and studies suggest that regularly changing or updating one's passwords could increase the password security of one's online accounts. Nowadays, it is recommended to regularly change one's password at least once or twice a year especially if one is not using two-form factor authentication (Gott 2018). This ensures safety of one's password even if a third party has gained access.

However, from ***Fig. 8***, it can be seen that 47% of all respondents changed their passwords only when required to do so, that is, if one could not remember one's password or if required by system etc. and 16% had never changed their passwords. From ***Fig. 9***, it can be seen that changing passwords only when required to do so is a popular choice across all the different population types studied. It is noted that people who are 65 years and above are less likely to change their passwords unless required to do so and thus, can be considered to be the most vulnerable group surveyed. It has been suggested by various authors that websites should send a reminder to their users to change their passwords once in a while, but it has also been studied that users tend to get annoyed when forced to change their passwords.

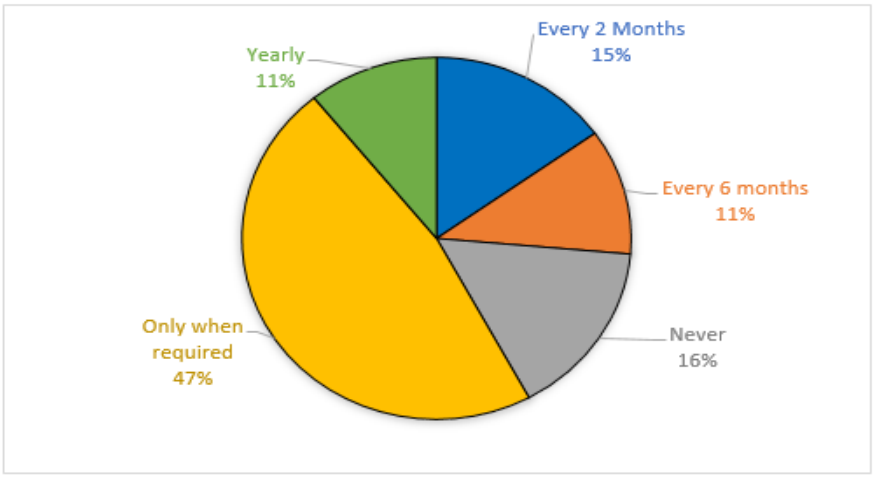

***Fig. 8**. Frequency of changing passwords*

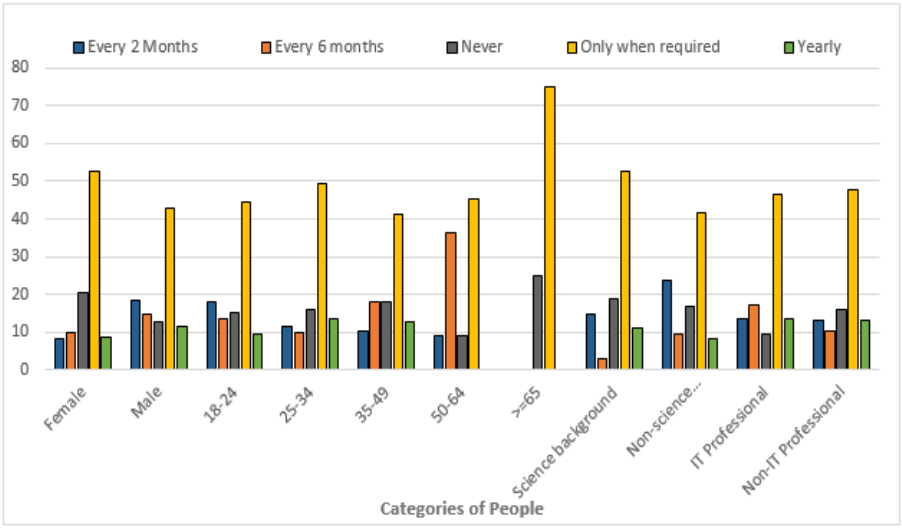

Fig. 9*. Frequency of changing passwords in percentage among the various groups of people*

TWO-FORM FACTOR (2FA) USAGE

2FA is a type of authentication technique that allows a user to gain access to his or her online account only after providing a combination of at least two pieces of information about what he or she knows (e.g. password, security question), has (identification card, mobile phone) or is (biometric property e.g. finger print). An example of a 2FA can be a pair of passwords and a one-time password (OTP) sent to the mobile phone.

Fig. 10 shows that only 48% of the population surveyed use some form of 2FA with their online accounts. What is more alarming to note is that 28% of the respondents are not aware of 2FA and another 24% who are aware choose not to use this with any of their accounts.

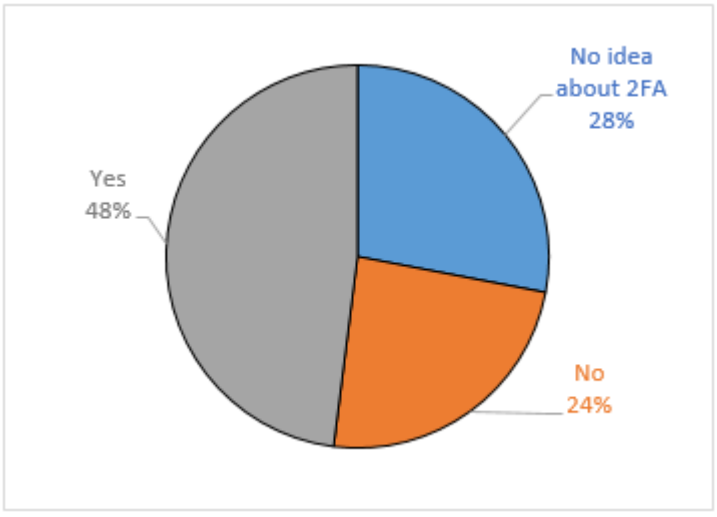

Fig. 10. *Use of 2FA among the respondents*

Fig. 11 shows that a higher percentage of respondents from each group of people surveyed do not use 2FA except those with some IT background, though it is still far from satisfactory even with this category of people. This shows that people need to be made aware of the importance of 2FA which gives an extra level of protection in addition to having good password practices.

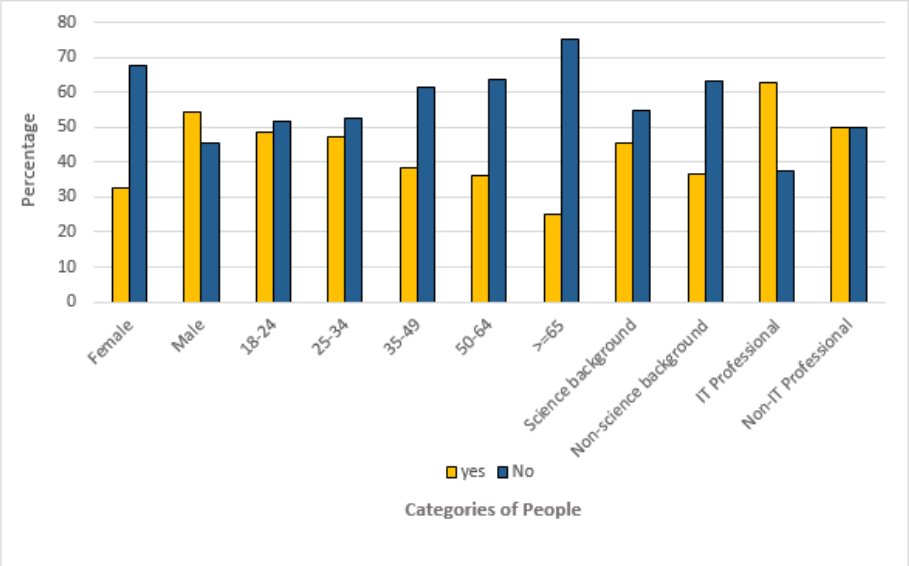

Fig. 11. *Use of 2FA among the various categories of respondents*

PASSPHRASE USAGE

Passphrase is a form of password with some techniques involved that make them stronger, sometimes longer, easier to remember and more secured. The key is to use a sentence or phrase that would be easy to remember but at the same time difficult for others to guess. Also, these phrases could be tweaked e.g. using only the first letters of every word in the phrase and also varying the use of cases and punctuation marks. For example, a passphrase could be **I l0v3 8ur93r5& Ch!p5** which would be easy to remember as it is personal and also difficult for others because of the combination and style of representation. Another representation of passphrases could be **!L8&c0@rd** (for **I l**ove **b**urgers **a**nd **c**hips **o**n **a r**ainy **d**ay).

The use of passphrase has been noticed to be significantly low among the respondents. Only about 21% of the total respondents have ever used passphrases, 79% have never used passphrases, of which 41% have never heard about passphrases.

From ***Fig. 12*** it can be seen that as age increases, the use of passphrases decreases. Also, those with an IT background or profession have a higher percentage of usage but it is still insignificant.

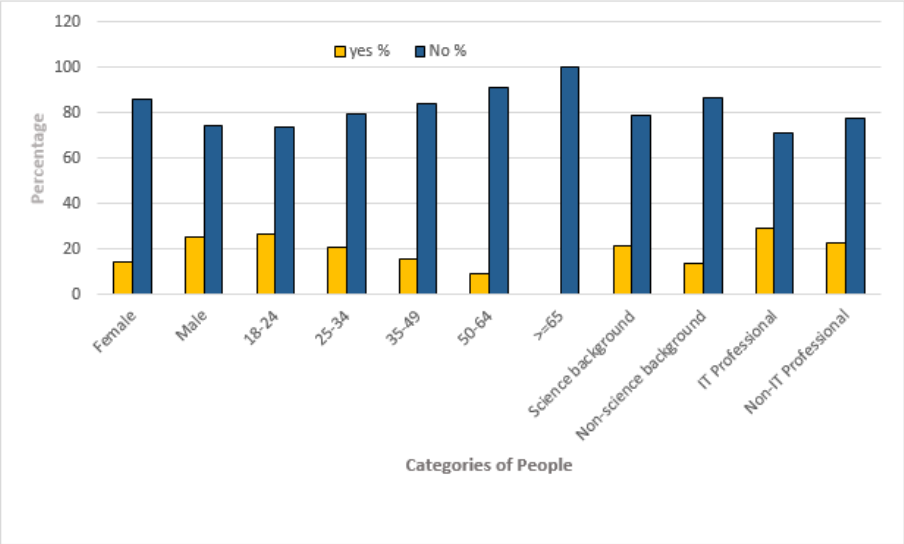

Fig. 12. *Passphrase use among the different population types*

ACCOUNT COMPROMISE

From the survey, it was found that 30% of the respondents had their online accounts compromised at least once in their lifetime. This, in essence, means approximately one in every three persons is vulnerable to account breach and this is a serious issue from a security point of view.

Fig. 13 shows that the groups of people who have experienced the highest number of account breaches are the males (91%) and those who are 65 years and above (100%). This could attribute to the fact seen earlier that the age group of 65 years and above either never changed their passwords or changed it only when required, shared it with others or might have used numbers or words which have significant importance to them. This would allow a hacker to profile a user and access the account easily. It is also interesting to note that 80% of the female population have either never experienced a breach in their account or suspected so.

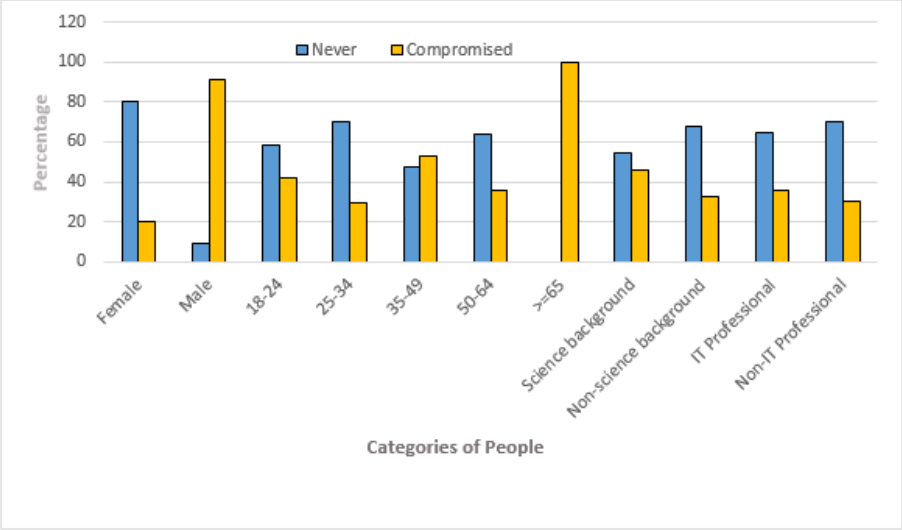

Fig. 13. *Percentages of Accounts breached across the different categories of respondents*

CONCLUSION

This study shows that even though online passwords have been actively used for over 20 years, the security practices and awareness are still seriously lacking. The age group of 65 years and above were found to be the most vulnerable group as it was seen that 100% of the group had their accounts compromised, followed by the male participants with a 91% of accounts compromised. It is worthy to note that 80% of the female population have either never experienced a breach in their account or do not have any idea if their accounts have been breached.

It was seen that 90% of the participants used words or numbers related to dates, phone numbers or names which had a personal significance or importance in their lives. These are easily remembered, but are highly discouraged as it can be used for profiling or stalking and making a password vulnerable to attack. It was also seen that out of 500 participants, 63% were vulnerable to password attacks as it includes people who never change their password or change it only when asked to do so; 23% would prefer passwords that were easy to remember; 53% would prefer secure passwords; while 24% would like their passwords to be easy and secure at the same time. In practice, however, it may not be feasible to implement easy to remember passwords that are secure at the same time. To achieve this, awareness should be created among users on the use of passphrases, password managers and multi-form factor authentication techniques which would improve online security.

ACKNOWLEDGEMENT

The authors thank all the respondents who participated in the survey and made it possible to carry out the research.

REFERENCES

1. Anonymous. 2019. “Bangladesh Telecommunication Regulatory Commission.” 2019. http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-february-2019.
2. Armerding, Taylor. 2018. “The 18 Biggest Data Breaches of the 21st Century.” CSO. 2018.
3. Awad, Mohammed, Zakaria Al-Qudah, Sahar Idwan, and Abdul Halim Jallad. 2017. “Password Security: Password Behavior Analysis at a Small University.” *International Conference on Electronic Devices, Systems, and Applications*, 3–6.
4. CISCO. n.d. “What Is Cybersecurity?” Accessed January 21, 2019. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.
5. Florencio, Dinei, and Cormac Herley. 2007. “A Large-Scale Study of Web Password Habits.” *Proceedings of the 16th International Conference on World Wide Web - WWW ’07*, 657.
6. Gaw, Shirley, and Edward W. Felten. 2006. “Password Management Strategies for Online Accounts.” In *Proceedings of the Second Symposium on Usable Privacy and Security - SOUPS ’06*, 44. New York, New York, USA: ACM Press.
7. Gott, Amber. 2018. “How Often Should You Change Your Password?” 2018. https://blog.lastpass.com/2018/08/often-change-password.html/.
8. Hamidur. 2009. “Internet History of Bangladesh.” 2009. http://wirelessbangladesh.blogspot.com/2009/04/internet-history-of-bangladesh.html.
9. Klein, Daniel V. 1992. “Foiling the Cracker: A Survey of, and Improvements to, Password Security.” *Programming and Computer Software* 17 (3): 5–14.
10. Lamport, Leslie. 1981. “Password Authentication with Insecure Communication.” *Communications of the ACM* 24 (11): 770–72.
11. Morris, Robert, and Ken Thompson. 1979. “Password Security: A Case History.” *Communications of the ACM* 22 (11): 594–97.
12. Raza, Mudassar, Muhammad Iqbal, Muhammad Sharif, and Waqas Haider. 2012. “A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication.” *World Applied Sciences Journal* 19 (4): 439–44.
13. Riley, Shannon. 2006. “Password Security: What Users Know and What They Actually Do.”

Usability News 8 (1): 2833–2836.

14. Shay, Richard, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2010. "Encountering Stronger Password Requirements : User Attitudes and Behaviors Categories and Subject Descriptors." *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10*, 1.
15. Techopedia. n.d. "Password." Accessed January 22, 2019. https://www.techopedia.com/definition/4042/password.
16. Tsokkis, Pieris, and Eliana Stavrou. 2018. "A Password Generator Tool to Increase Users' Awareness on Bad Password Construction Strategies." *2018 International Symposium on Networks, Computers and Communications, ISNCC 2018*, 1–5.