

User Privacy & Security in Internet: A Concern for Bangladesh

Asif Hossen Nipun

Roll: ASH1701052M

Year : 4, Term : 2

22 February, 2022

A Thesis

**Submitted for partial fulfillment for the Bachelor
Degree**

Supervisor

Md Javed Hossain

Associate Professor

**Department of Computer Science and
Telecommunication Engineering**



Noakhali Science and Technology University

Acknowledgement

I would like to thank my thesis supervisor ***Md Javed Hossain***, Associate Professor, Department of Computer Science and Telecommunication Engineering, Noakhali Science and Technology University. He inspired me by giving valuable guidance, time and supervises my working progress. It is completely impossible to develop this thesis without his motivation and help.

Finally, All praise to my Lord. I would like to thank almighty ALLAH who gives me the patient to do such a research like **User Privacy & Security in Internet: A Concern for Bangladesh**

Declaration

I, **Asif Hossen Nipun**, student at Department of Computer Science and Telecommunication Engineering, Noakhali Science and Technology University, hereby submit this thesis report in partial fulfillment of the requirements for the award of degree of BSc in Engineering in CSTE. I have not plagiarized or submitted the same work for the award of any other degree.

Asif Hossen Nipun

Certification

This is to certify that as fulfilment of the partial requirement for completing the thesis on “**User Privacy & Security in Internet: A Concern for Bangladesh**”, Asif Hossen Nipun, CSTE 4th year student at Department of Computer Science and Telecommunication Engineering, Noakhali Science and Technology University, has completed the same under my guidance and submitted it to the department as per ordinance of CSTE. It is an authentic work of the student and fit for evaluation.



Md Javed Hossain

Associate Professor

Department of Computer Science
and Telecommunication Engineering

ABSTRACT

Social engineering is an attack vector that primarily focuses on human interaction and typically includes persuading individuals to violate traditional security policies and best practices in order to gain unauthorized access to systems, networks, or physical locations, or for financial gain. In our nation, Bangladesh, a big number of individuals use the internet for a variety of purposes such as social media, e-banking, entertainment, and other forms of communication. A breach in their security can compromise a vast quantity of data security, causing consumers to suffer emotionally and financially. The study focuses on the most widely used passwords across a variety of websites on the internet. Internet users in Bangladesh are not as well educated in terms of password usage, since they rely on obvious passwords to safeguard their accounts. A substring of their phone number, in particular, is a recognizable password to a substantial share of users, posing a security risk. Our study's goal is to learn about the current architecture of user security, identify potential breaches in security architecture, and raise awareness among relevant authorities in order to implement appropriate security measures for Bangladesh's internet users.

Keywords: Social Engineering Attack, Internet Security in Bangladesh, Same Password in Several sites, Common Password Uses

Table of Contents

Acknowledgement	2
Declaration.....	3
Certification.....	4
ABSTRACT.....	5
Chapter 1	8
Introduction.....	8
1.1 Introduction.....	8
1.2 Motivation.....	8
1.3 Objectives	9
1.4 Expected Outcome	9
Chapter 2	10
Related Works.....	10
2.1 Security aspects in using Social networks	10
2.2 Security aspects in using E-banking	12
2.3 Miscellaneous	13
Chapter 3	14
Research Methodology	14
3.1 Secondary Data Overview	14
3.2 Primary Data Overview	15
3.3 Online Survey Details	16
3.4 Resources of the Study.....	17
3.5 Data Mining and analyzing method	17

Chapter 4	18
Results Analysis.....	18
4.1 Survey Data analysis.....	18
4.2 Output	21
Chapter 5	22
Conclusion & Future Work	22
5.1 Introduction.....	22
5.2 Conclusion	22
5.3 Future work.....	22
References.....	23

Chapter 1

Introduction

1.1 Introduction

In Bangladesh, a huge amount of people of different classes are connected to internet for various reasons. Protecting the privacy & security of their personal information is the most important topic for the concerned authority. The statistics shows that cybercrimes are increasing rapidly throughout Bangladesh. User privacy is not protected & security measure is also miserable in most of the websites and online applications. Big companies like Facebook, Google and Microsoft are giving prime concern to the user security and privacy. But sometimes users are losing their data security for their own mistakes and by falling in trap created by bad guys of internet. The mass people of the country are not adaptive with the new concept of security measure.

1.2 Motivation

We have experienced many Bangladeshi internet users who uses their name, birth date, phone number or part of phone number as their password. They also use it in so many aspects. This is a potential risk of being attacked by Social Engineering hacking method. Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. It also refers to the psychological manipulation of people into performing actions or divulging confidential information. Our research is to analyze these kind of vulnerability of Bangladeshi internet users.

1.3 Objectives

- To analyze the vulnerability of the users of Bangladesh in using internet password.
- To determine the primary target of social engineering attack.
- To raise consciousness about being safe in cyber world.

1.4 Expected Outcome

As far as our motivation of the research is concern, using easy and common password in various site is very much available in our users [15][16]. Hopefully, we will get something more suited in social engineering aspect that gives us more accurate analysis ability and results.

Chapter 2

Related Works

Although there are several area of using internet, users are primarily adopted with Social networks, E-banking, Entertainment, Communication and Education etc. Concerning Social network, there are a huge amount of users are connected with internet. A large amount of information of every users are collected by these social networking sites. As E-banking is increasing day by day, financial security and privacy is also a big challenge. By getting hacked, a user is confined with so many self-related information and also financial loss. Following are some areas of works done based on social engineering aspects related to E-banking, social networking and other aspects of internet uses.

2.1 Security aspects in using Social networks

The users in Bangladesh are not so much educated in online media area. Though the organizations are providing much features and private life in social media, the less knowledge about using the sites of users is a big security issue. According to a study named “Social Engineering Attacks on Facebook – A Case Study” done recently shows that 46 percent of Facebook users are not confined to rely upon Facebook for their privacy or personal information concern. The study was conducted in 2019 with 1123 American users [10]. Social engineering attacks are based on user vulnerability. Vulnerable users are more suitable for being attacked. Some other studies are:

Cyber Threat and Security: Bangladesh Perspective

Cybercrime may pose a threat to any country's national security, but Bangladesh is particularly vulnerable to this sort of attack. Because of a lack of modern cyber technologies and a lack of knowledge, the country may face a severe security danger as a result of cybercrime. Furthermore, the present cyberspace laws are ineffective in protecting the country's cyberspace. To deal with the cyber security issue and its usage in transnational organized crime, Bangladesh need increased international collaboration, technological know-how and competence, and widespread public awareness. Many of us may argue that cyber risks are not a likely scenario for Bangladesh in the

near future, but we cannot ignore the existing facts about the rise of cybercrime in both Bangladesh and the rest of the globe.[1]

Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh

According to previous study on technology use in the Global South, people in disadvantaged areas commonly share a single device among numerous persons. However, the data privacy issues and conflicts that develop when individuals share gadgets have not been thoroughly researched [2]. This article describes the findings of a qualitative research with 72 participants that examined how families in Bangladesh now share mobile phones, their usage patterns, and the tensions and obstacles that develop when individuals want to safeguard the privacy of their personal data. We demonstrate how individuals share electronics not only for economic reasons, but also because sharing is a social and cultural activity that is strongly ingrained in Bangladeshi society.

Data Privacy in Bangladesh A Review of Three Key Stakeholders Perspectives

The research focuses on data privacy in Bangladesh. The study's goals are threefold: first, to understand consumers' perspectives on the importance of data privacy; second, to understand industry experts' perspectives on data privacy; and third, to examine governments' stakes and actions to safeguard personal data. This study examines the present state of data privacy in Bangladesh and makes recommendations to improve data protection in the country [3].

Cyber security in the globalized world: challenges for Bangladesh

With the increased global adoption of information and communication technology, cybercrime looks to be a possible danger to sensitive computer data and systems. This crime is also committed in technologically sophisticated countries like as the United States. Bangladesh, being a developing country, is vulnerable to cybercrime, which undermines the country's national security. The present government's Digital Bangladesh strategy is to guarantee internet access in all governmental institutions by 2021[4].

2.2 Security aspects in using E-banking

According to a research titled "Security of E-Banking in Bangladesh," 34% of respondents are from rural areas, 40% are from municipalities, 17% are from various district towns, and 29% are from city corporations. 15 percent of respondents from diverse places stated that internet banking is extremely secure. According to 15% of respondents, e-banking in Bangladesh is extremely secure, while 31% believe e-banking security in Bangladesh is inadequate. 11.5 percent of all respondents are unaware of the security status of e-banking in Bangladesh. 31.7 percent of those polled use some numbers as a password. 13.3 percent use either their name or a letter, 18.3 percent use a combination of digits and letters, and 28.33 percent do not have e-banking accounts[7][18].

A framework for the mobilization of cyber security and risk mitigation of financial organizations in Bangladesh: a case study

This thesis was designed to provide a current scenario of cyber security among financial organizations in Bangladesh, as well as to answer some critical questions such as how an organization becomes aware of different cyber risks or data breaches by analyzing cyber enabled services, how they should plan to protect their assets or customers, what the major challenges are in setting up cyber security, and how organizations can prevent or mitigate the risks associated with cyb The study also analyzed material authored by scholars all over the world on cyber security of financial institutions, hacking incidents, threats, cyber effect on financial businesses, risk measurement, prevention, and mitigation, and so on[5].

2.3 Miscellaneous

According to a research titled "Why Do People Adopt, or Reject, Smartphone Password Managers" done by Nora Alkaldi and Karen Renaud, relatively few people can use password managers to generate and store passwords. A few people have picked safe password manager [11] from among them. According to the survey, just 33% of iPhone users have employed Touch ID for security measures, indicating that people are not aware with or informed about current security procedures [8]. They are not in excellent command of establishing several passwords for different websites [13][17]. Users are also hesitant to create passcodes that include upper and lower case letters, numbers, and alphanumeric symbols [12].

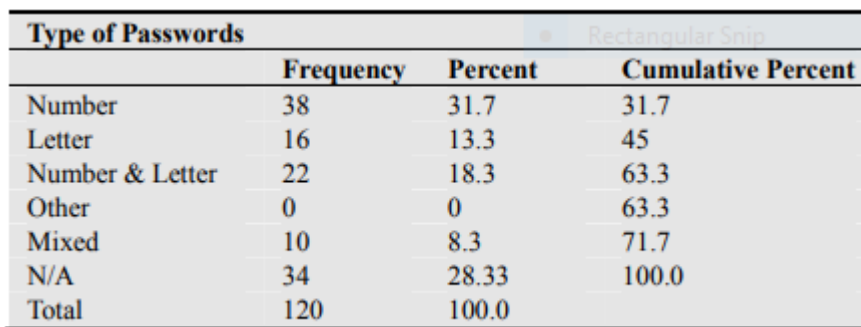
Chapter 3

Research Methodology

Our research consists of reading relevant publications and gathering data and information about them, collecting quantitative data, analyzing the data using various methods, and going through the predicted results of our research. The research begins with a review of more than 20 research articles on our topic. According to research, internet users are not concerned with the privacy of their personal information and often use the same password across many sites [6]. Users are unfamiliar with the process of constructing a password that includes letters, numbers, special characters, and so on. They also utilize popular passwords that include Name, Birth Date, Phone Number, Social Identity Number, Passport Number, and a vast number of patterns and easy-to-remember passwords, among other things. Our Bangladeshi users, in particular, share their passwords and PINs.

3.1 Secondary Data Overview

In aspects of E-banking mentioned before the Authors of “Security of E-Banking in Bangladesh” stated a high vulnerability of the users. Following are some data diagram from the journal.



Type of Passwords	Frequency	Percent	Cumulative Percent
Number	38	31.7	31.7
Letter	16	13.3	45
Number & Letter	22	18.3	63.3
Other	0	0	63.3
Mixed	10	8.3	71.7
N/A	34	28.33	100.0
Total	120	100.0	

Fig 1: Type of Passwords Used by the Respondents for Maintaining E-Bank Account.

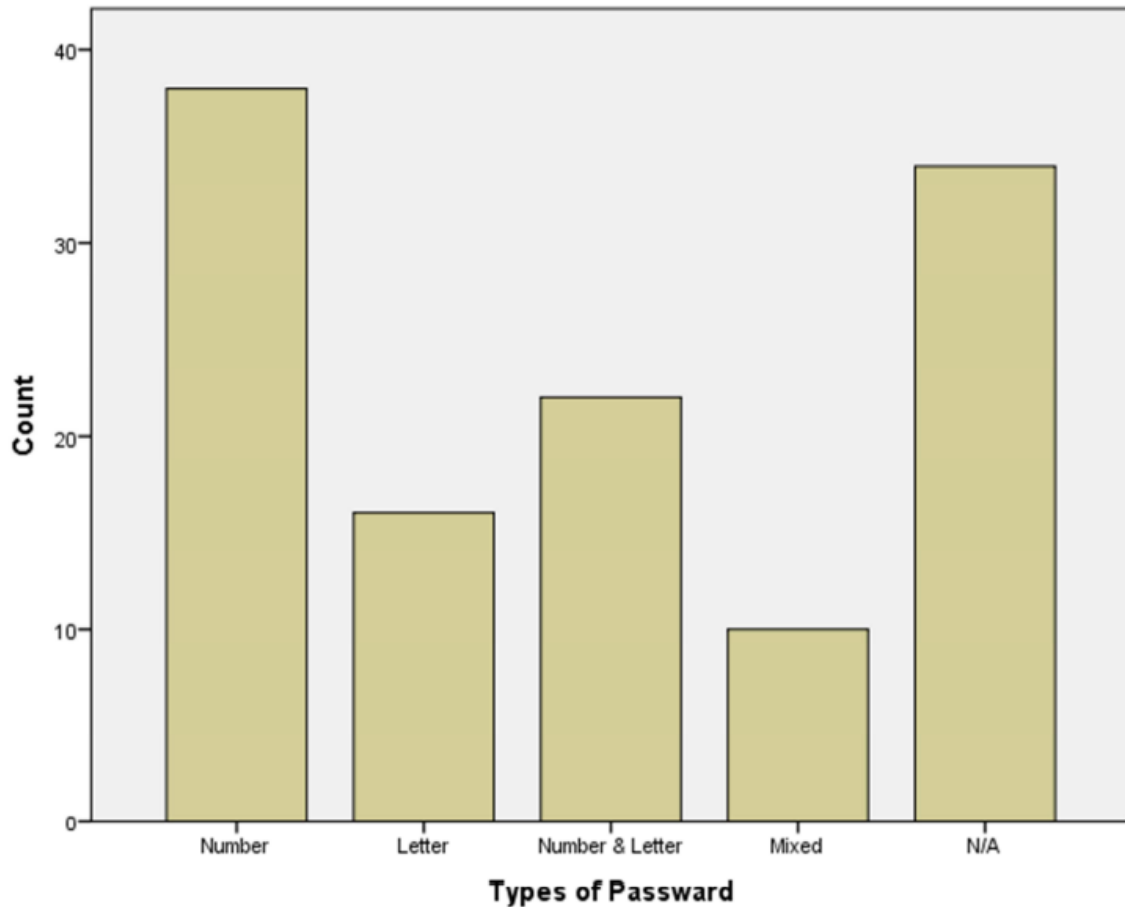


Fig 2: Type of Passwords Used by the Respondents to Maintain E-Account.

The study briefly mentioned that 31.7 percent of those polled use some numbers as a password. 13.3 percent use simply their name or a letter, 18.3 percent use a combination of digits and letters, and 28.33 percent do not have e-banking accounts!

3.2 Primary Data Overview

We have done online survey among users of various classes and standards for attaining the problems they faced about privacy topic under their experience on internet. The survey is conducted among University students including Noakhali Science & Technology University, Barisal University and Premier University Chattogram to get student view of internet security issues. There is also another survey conducted in a miscellaneous users of internet. We have got

help from using Google Forms in this measure. There will be testing and examining the popular websites to achieve the security measure. The survey consist of five questions with having multiple choice answering system. Users were able to give more than one answer per question in multiple answer aspects.

3.3 Online Survey Details

We have conducted two different survey by using Google Forms. One is for only among university students and other is for miscellaneous purpose. There were a great response among users and we have got almost 300 individual internet user data by conducting the surveys.



User Privacy & Security in Internet: A Concern for Bangladesh Survey || January, 2022 || University

Don't need to hesitate in giving information as you are giving information anonymously.
No need to provide your name, email, contact number etc in the form.
Thanks in advance for helping us.

Often forget your password ? *

☐ Yes (হ্যাঁ)

☐ No (না)

Do you use same password in several sites ? *

☐ Often (প্রায়ই)

☐ Hardly (খুব কমই)

Fig : Survey screeshot

3.4 Resources of the Study

- Google Forms for Data Collection
- Google spreadsheet for Data storing
- Microsoft Excel for Table data overview and storing
- Jupyter Notebook for live code, educational and computational output and visualization
- Python codes for data mining, reshaping and analyzing
- Microsoft Word for Documentation and overview

3.5 Data Mining and analyzing method

Python Command list in Jupyter Notebook

```
In [40]: import numpy as np
import pandas as pd
import os
import random
import scipy.stats as st

%matplotlib inline

import matplotlib as mlt
import matplotlib.pyplot as plt
import seaborn as sns

plt.style.use('ggplot')
```

```
In [41]: DATASET_PATH = ''

def load_the_dataset(file_name, dataset_path=DATASET_PATH):
    csv_path = os.path.join(dataset_path, file_name)
```

```
Out[59]: No      ( ना )      48
         Yes      ( हा )      38
         Name: Strong_Password_Usage_?, dtype: int64
```

```
In [60]: dataset.replace({'Strong_Password_Usage_?': {
         'No      ( ना )': 'No', 'Yes      ( हा )': 'Yes',
```

```
In [61]:
```

```
Out[61]: No      48
         Yes      38
         Name: Strong_Password_Usage_?, dtype: int64
```

Fig : Screenshot of Python commands in Jupyter and outputs

Chapter 4

Results Analysis

4.1 Survey Data analysis

The survey was conducted among university students and miscellaneous internet users. Two different Google form provided us total of 291 individual internet user data where 258 was among university students and other from the user out of the university. Following are some figures of the data we have achieved.

Forget_Password_?	Same_Password_In	Strong_Password_Usage_?	Obvious_Passwords_Usage_?	Password_Strength
Yes	Never	No	Mobile No	strong enough
Yes	Often	No	Part of Mobile No	Not strong enough
Yes	Often	No	Mobile no, Name	strong enough
Yes	Often	Yes	None of the above	Not strong enough
No	Hardly	Yes	Name	strong enough
Yes	Often	Yes	None of the above	Highly strong
Yes	Hardly	No	None of the above	strong enough
Yes	Often	No	None of the above	strong enough
No	Hardly	Yes	Name	strong enough
Yes	Often	No	None of the above	strong enough
No	Hardly	Yes	None of the above	strong enough
Yes	Often	Yes	Part of mobile no	strong enough
Yes	Often	No	None of the above	Not strong enough
Yes	Hardly	No	Mobile no	strong enough
Yes	Often	No	None of the above	strong enough
No	Often	No	Part of Mobile no	Not strong enough
Yes	Hardly	Yes	Mobile no	strong enough
Yes	Often	No	None of the above	strong enough
Yes	Often	Yes	Mobile no	Not strong enough
No	Never	No	Part of Mobile no	strong enough
Yes	Often	Yes	Part of Mobile no	strong enough
No	Never	Yes	Part of Mobile no	strong enough
No	Hardly	Yes	None of the above	strong enough
Yes	Hardly	Yes	Part of Mobile no	strong enough

Fig: A portion of the dataset

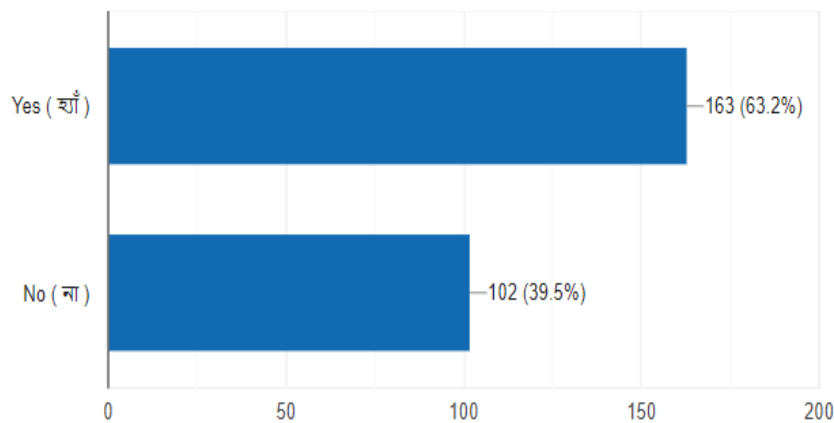


Fig : Percentage of people often forget their password

The chart shows that People often forget their password. From the data, we have acknowledged that more than 63 percent of people often forget their password. And for this reason they use same password in several sites. The following figure shows that 57 percent of the university internet user use a password in several sites and out of the university almost 55% of the users use same password in multiple sites they need to. The study also states that more than 33% of the university users and 18% of miscellaneous people hardly use same password in several sites.

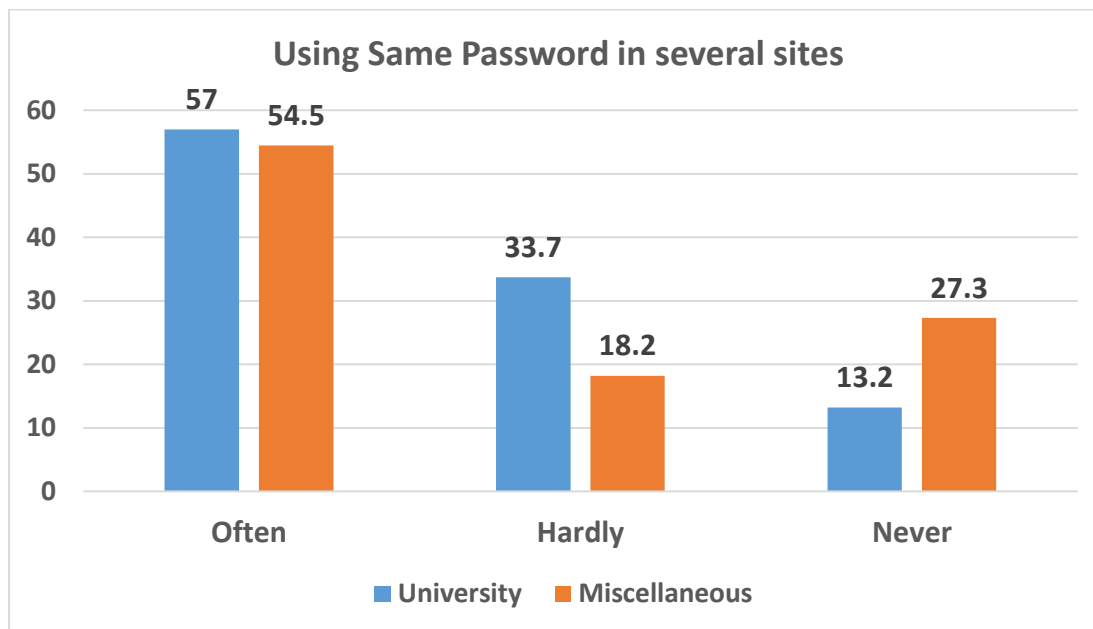


Fig: Percentage of using same password in several sites

Area of Studies	University	Miscellaneous
Part of Mobile Number	90 (34.9 %)	12 (36.4%)
Mobile Number	41 (15.9 %)	0 (0%)
Name	113 (43.8 %)	9 (27.3 %)
Birth Date	42 (16.3%)	3 (9.1 %)
None Of These Above	82 (31.8 %)	12 (36.4%)

Fig:Type of Passwords used by internet users in Bangladesh

The table of data shows that above 50 percent of the university participant uses or used a password containing mobile number or part of mobile number. Password containing Name of the users was 44 percent. 16 percent stated that they had used their birth date as password. 31 percent users reported that they never used these sorts of passwords. On the other hand , outside of the university participant states that 36 percent of the internet users use part of their phone number as passwords. 27 percent of them used Name as Passcode and 36 percent never use any of these.

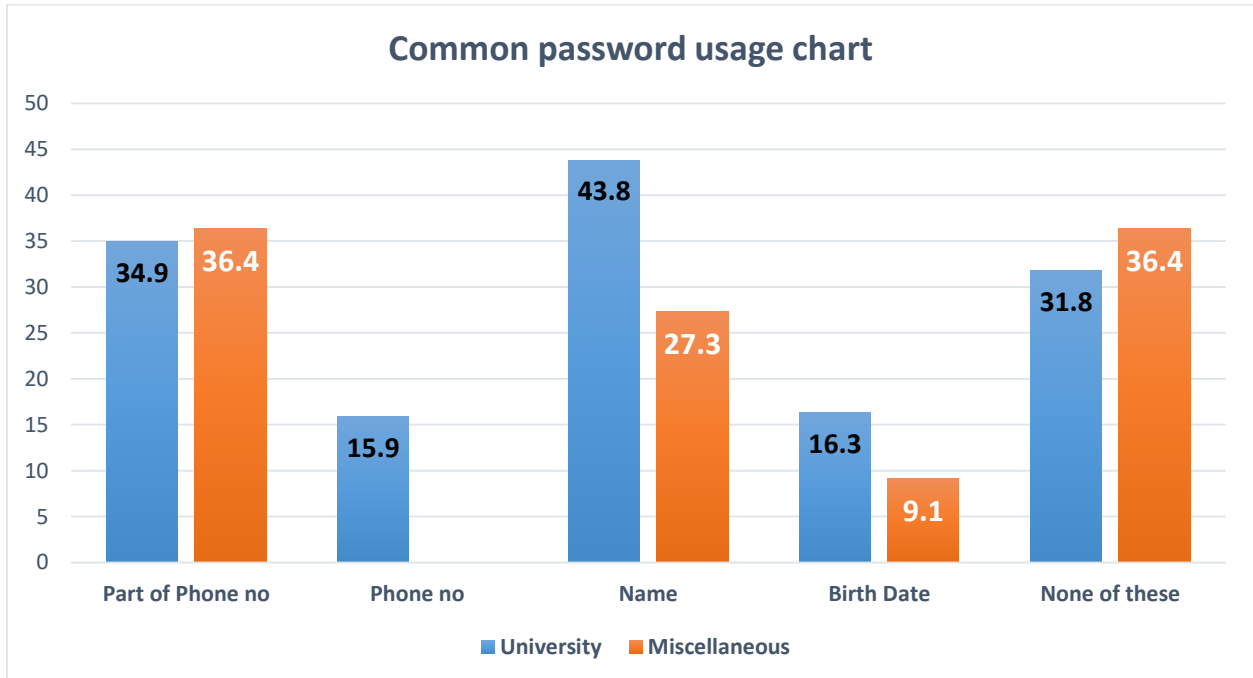


Fig : Common password usage chart

4.2 Output

According to the poll results, people are quite familiar with using phone numbers, substrings of phone numbers, birth dates, names, and so on as passwords. However, the data quickly explains that almost half of people, or 50%, use simply a phone number or a portion of a phone number as their password. Users utilize this readily guessable and weak password method on social networking sites [22], financial security, and other elements of internet use [19]. As we have seen, the component of the phone number is nothing more than the final six digits of the phone number. Furthermore, Bangladeshi consumers prefer to use the last six digits of their phone number as their password. According to our research, major social networking sites are utilized by a large number of individuals. In Bangladesh, there are a lot of people who use the internet for things like Facebook, Tik-Tok, Google, and Instagram. A large number of individuals are also connected to E-banking and Mobile Finance System. As a result, a flaw in password usage can pose a significant risk to this broad population of people. A social engineering assault that takes advantage of a person's weakness might result in massive data loss and financial hardship for the individual.

Chapter 5

Conclusion & Future Work

5.1 Introduction

Attacks on social media platforms, such as Facebook, LinkedIn, Twitter, and Instagram, target sites with significant user populations. The bulk of recent assaults, which are patterned after the earlier Koobface virus, simply employ social media sites as a delivery mechanism. Researchers currently believe that sophisticated assaults on social media networks will be able to exploit a user's relationships, location, and even commercial operations. This data may then be used to create targeted advertising campaigns for individual people, or it can even be used to incite crime in the virtual or real world[21].

5.2 Conclusion

From our experience in this research, we have deeply acknowledged that users of internet in Bangladesh are familiarly occupied with using digit based password. Specially, Phone number is the high in using probability. Our new invention is that they uses the last 6 digit of phone number as their password. This is a huge risk for our country internet users for future as attackers may attack them by knowing vulnerability of the users. We want to conclude the proper authority in this scope to be conscious in this manner and to protect our users in this networking medium. Provide the best privacy & security should be the most important factor as there are a huge part of population is under internet service. Giving the perfect online environment will make society developed and conscious which is good for all sorts of internet users. We have done hard struggle to make a great research and to help Bangladesh.

5.3 Future work

Our research have some limitations as our data mainly collected from the young users. Future work should be done under a large diversity of users to get more accurate results. Also pattern based password using survey can be done under this topic as people are very familiar with pattern based password using. If the part of phone number is a pattern then users will use this as password that is highly possible [20]. This is a good opportunity of research.

References

1. Mahmuda Akhter Bonnya, “Cyber Threat and Security: Bangladesh Perspective”, IOSR Journal Of Humanities And Social Science (IOSR-JHSS) , Volume 25, Issue 3, Series. 8 (March. 2020) 19-28 e-ISSN: 2279-0837, p-ISSN: 2279-0845. www.iosrjournals.org
2. Syed Ishtiaque Ahmed, Md. Romael Haque, Jay Chen, Nicola Dell, “Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh”, Proceedings of the ACM on Human-Computer Interaction, Volume : 1, Issue No : CSCW, Article No : 17, December 2017, <https://dl.acm.org/doi/10.1145/3134652> .
3. Kamal Hossain, Khabirul Alam, Umme Sara Khan, “Data Privacy in Bangladesh A Review of Three Key Stakeholders Perspectives”, Conference: Seventh International Conference on Advances in Social Science, Economics and Management Study - SEM 2018, 10.15224/978-1-63248-164-1-32, October, 2018, shorturl.at/horOU .
4. Mohammed Nur Nabi, Mohammed Tanjimul Islam, “Cyber security in the globalized world: Challenges for Bangladesh”, Conference: Economic and Social Development, 7 th International Scientific Conferenc, At: New York, USA, October 2014, shorturl.at/hsEW7 .
5. Md Nurul Afser Siddique, “A framework for the mobilization of cyber security and risk mitigation of financial organizations in Bangladesh: a case study”, Department of Industrial and Production Engineering, Bangladesh University of Engineering and Technology in partial fulfillment of the requirements for the degree of Master of Engineering (M. Engg.) in Advanced Engineering Management (AEM), shorturl.at/dlNY2 .
6. Abdul Shareef, Pallivalappil, Jagadeesha, S. N., & Krishna Prasad, K., (2021). Social Engineering Attacks on Facebook – A Case Study. International Journal of Case Studies in Business, IT, and Education (IJCSBE), 5(2), 299-313. DOI: <https://doi.org/10.5281/zenodo.5765883>
7. Mohammad Shamsus Sadekin, Md. Abdul Hannan Shaikh. Security of E-Banking in Bangladesh. Journal of Finance and Accounting. Vol. 4, No. 1, 2016, pp. 1-8. doi: 10.11648/j.jfa.20160401.11
8. Alkaldi, N. and Renaud, K., 2016. Why do people adopt, or reject, smartphone password managers?

9. Google drive Link for dataset of spreadsheet : shorturl.at/dlpvC, 21.02.2022.
10. Pallivalappil, A.S. and Jagadeesha, S.N., 2021. Social Engineering Attacks on Facebook—A Case Study. *International Journal of Case Studies in Business, IT and Education (IJCSBE)*, 5(2), pp.299-313.
11. Alkaldi, Nora, and Karen Renaud. "Why do people adopt, or reject, smartphone password managers?." (2016).
12. Yampolskiy, R.V., 2006, October. Analyzing user password selection behavior for reduction of password space. In *Proceedings 40th annual 2006 international carnahan conference on security technology* (pp. 109-115). IEEE.
13. Das, A., Bonneau, J., Caesar, M., Borisov, N. and Wang, X., 2014, February. The tangled web of password reuse. In *NDSS* (Vol. 14, No. 2014, pp. 23-26).
14. All dataset of the thesis : <https://drive.google.com/drive/folders/1WnINBPOzSXHevTA8iZ7kFYuhcWwwdMJX?usp=sharing> , 21,02,2022.
15. Yampolskiy, R.V., 2006, October. Analyzing user password selection behavior for reduction of password space. In *Proceedings 40th annual 2006 international carnahan conference on security technology* (pp. 109-115). IEEE.
16. Wang, D., Zhang, Z., Wang, P., Yan, J. and Huang, X., 2016, October. Targeted online password guessing: An underestimated threat. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 1242-1254).
17. Wash, R., Rader, E., Berman, R. and Wellmer, Z., 2016. Understanding password choices: How frequently entered passwords are re-used across websites. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)* (pp. 175-188).
18. Grawemeyer, B. and Johnson, H., 2011. Using and managing multiple passwords: A week to a view. *Interacting with computers*, 23(3), pp.256-267.
19. Herley, C., Van Oorschot, P.C. and Patrick, A.S., 2009, February. Passwords: If we're so smart, why are we still using them?. In *International Conference on Financial Cryptography and Data Security* (pp. 230-237). Springer, Berlin, Heidelberg.
20. Chou, H.C., Lee, H.C., Yu, H.J., Lai, F.P., Huang, K.H. and Hsueh, C.W., 2013. Password cracking based on learned patterns from disclosed passwords. *IJICIC*, 9(2), pp.821-839.
21. Beckers, K., Krautsevich, L. and Yautsiukhin, A., 2014. Analysis of social engineering threats with attack graphs. In *Data privacy management, autonomous spontaneous security, and security assurance* (pp. 216-232). Springer, Cham.
22. Algarni, A., Xu, Y. and Chan, T., 2017. An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. *European Journal of Information Systems*, 26(6), pp.661-687.