The Art of the Computer Passwords in Sri Lanka

Fernando W.P.K., Chathurangika S.D.J.
Faculty of Technology
University of Sri Jayewardenepura, Sri Lanka

Abstract - Passwords play an essential role in the sector of information security. A developing country like Sri Lanka with very low computer literacy is facing the challenge of securing its general public's digital privacy and security. Under these circumstances, responsible authorities and interested parties are more concerned about this matter and fondly anticipated towards an effective solution. This paper mainly discusses Sri Lankan's interaction with computer passwords, practical usage, and knowledge. The present study also focuses on passwords essentials, managing techniques, and new trends as well as the challenge of it.

Index Terms - authentication, computer passwords, digital accounts, digital privacy, digital security.

1 Introduction

The password is nothing new to this world. It has been around us for centuries. Way before the internet and computers, the passwords were used for military, intelligence, and security purposes. In 1961 Massachusetts Institute of Technology(MIT) developed an operating system called Compatible Time-Sharing System(CTTS), which was the first computer system that has the password login implementation [1]. Since then, passwords became the primary way to make access control and authentication to any computer information system.

With the rapid development and implementation of Information Technology throughout Sri Lanka, 'password' has become something significant, but its importance still stays hidden and silent. Among 21 million populations, we have around 7.2 million internet users in Sri Lanka, which has only 27.5% computer literacy. The question of how Sri Lankans engage with computer passwords remains at a very critical level. Among 7.2 million internet users, there is 6.5 million Face book (most popular social media platform in Sri Lanka) users and nearly 7 million Gmail (mostly used email service in Sri Lanka) users actively engaged [2].

2 Literature Review

A study was undertaken in 2017 to research the utilization and impression of Sri Lankan youth on the security and privacy aspects of the social networking sites through a survey conducted at INFOTEL 2017 exhibition hung in November focusing on the young people in the age gathering of 16-30 [3]. The study revealed that 81% of the youth is aware of the advanced security features of social networking sites. Still, many Sri Lankan young generations have been subject to different types of online victimization, such as getting hacked digital privacy breaches. The study also reveals a significant amount of survey participants has declared that they have disclosed their details on their digital accounts. Since this study was conducted targeting only the younger generation of our society, we can estimate that these numbers and studied decisions should have different resolutions when compares to the whole Sri Lankan society.

3 Methodology

This study adopts a quantitative research approach based on the comprehensive review of the literature; a survey instrument was developed with the use of Google Analytics tools and deployed through both electronic and paper-based format with a sample of 200 participants all over the country. Fig. 1 represents the age distribution of, and Fig. 2 represents the residency distribution of our survey participants.

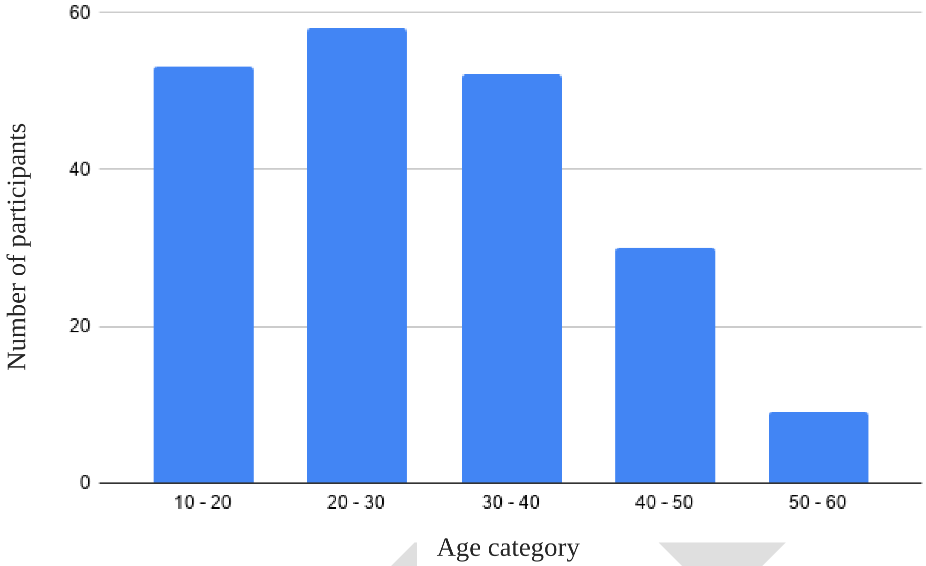

Fig. 1. age distribution of survey participants

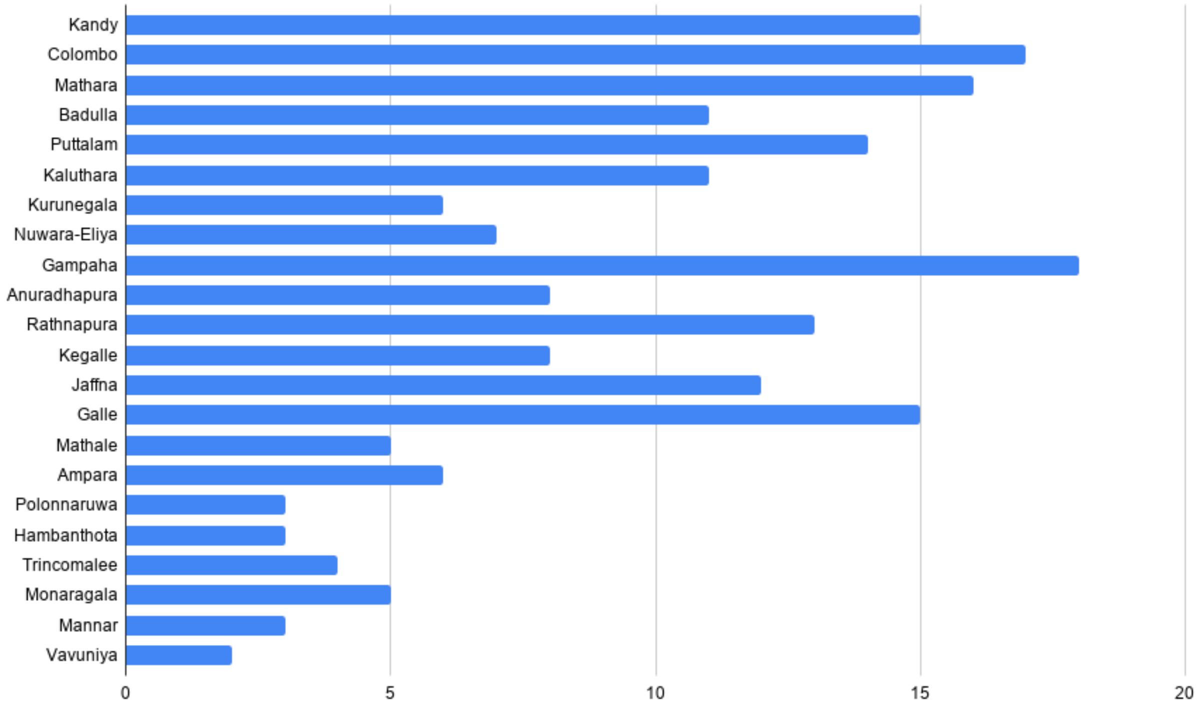

Fig. 2. residency distribution of survey participants

4 Passwords and Its Nature

Passwords are the main user authentication method that we use today in almost all the information systems. So every person should try to create a strong password that could not be easily guessed by anyone else, and they should be responsible for keeping their passwords confidentially. The majority of our society try to neglect the importance of the passwords when they are the best security mechanism to secure their digital life from intruders and cybercriminals. Fig. 3 represents choices of the survey responders when they were asked to choose a password from a given pool of passwords for their e-banking account.

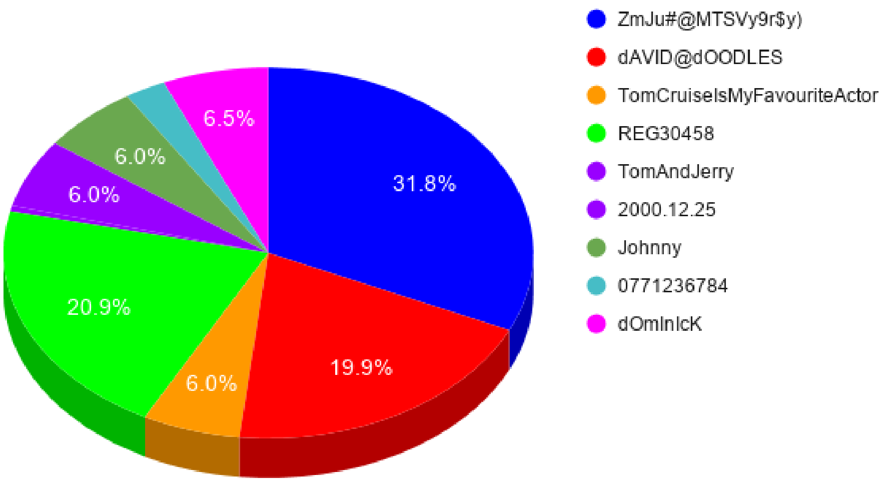

Fig. 3. Preferred password for an e-banking account

Users have the freedom to choose anything they desire as their passwords according to that particular information system rules and regulations. However, the best practice is to create a secure and memorable password; users might need to think creatively with something they are more familiar. It can be consist of and choose more than eight characters, mixed up with upper case letters, lower case letters, numbers, and special characters that are allowed. The most crucial aspect that you need to remember is not to use simple and less complicated passwords in any matter to avoid being hacked or cracked by quickly guessing or being a victim of a brute force attack (Table 1). Common passwords, keyboard patterns, personal details should be prevented from using in any matter. Table 1 shows how long it does take to crack a password with only numbers, upper or lower case letters only, Upper and lower case mixed, Numbers and letters, and Numbers, letters and symbols mixed along with a number of characters.

Table 1. Time taken to crack a password respective to the length [4]

No of characters	Only numbers	Upper or lower case letters only	Upper and lower case mixed	Numbers, letters	Numbers, letters and symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 seconds	10 seconds
6	Instantly	Instantly	8 seconds	3 minutes	13 minutes
7	Instantly	Instantly	5 minutes	3 hours	17 hours
8	Instantly	13 minutes	3 hours	10 days	57 days
9	4 seconds	6 hours	4 days	1 year	12 years
10	40 seconds	6 days	169 days	106 years	928 years
11	6 minutes	169 days	16 years	6000 years	71000 years
12	1 hour	12 years	600 years	108000 years	5 million years
13	11 hours	314 years	21000 years	25 million years	423 million years
14	4 days	8000 years	778000 years	1 billion years	5 billion years
15	46 days	212000 years	28 million years	97 billion years	2 trillion years

Another vital thing that research pointed was unawareness of password confidentiality in our general public. The essential characteristic of a password is confidential and not shared with anyone other than yourself. Fig. 4 is representing responses of survey participants about their password sharing among family, friends, etc. A significant amount of people in our society intends to share passwords among their family and friends. According to survey results, the majority is sharing passwords among spouses and couples. Sometimes very few even share passwords with total strangers that they meet online. Password sharing usually could be seen among women rather than men.

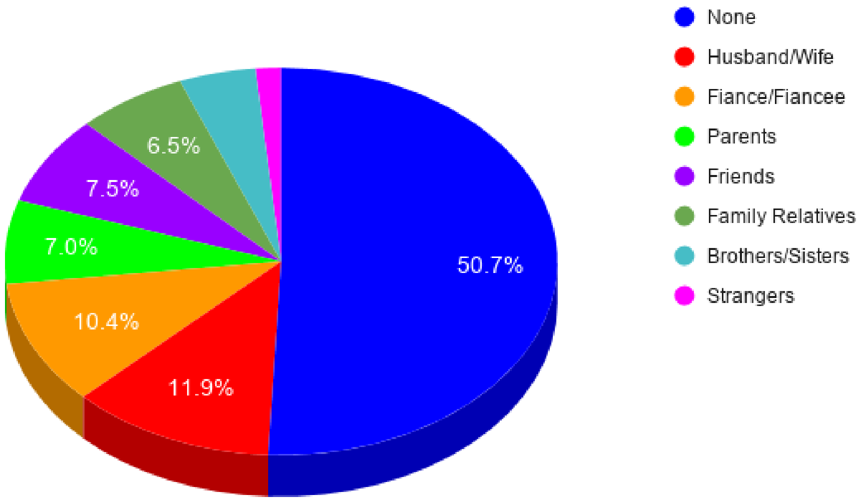

Fig. 4. Password sharing

In specific scenarios, unknown devices might have to be used to login to digital accounts without the usually trusted devices. The tragedy behind this is that they forget to check for possible security threats and log out from those devices after the job is done. Scenarios like that had led most of our internet users into a certain level of privacy exposure. In any suspicious activity or any possible leakage of digital privacy should be handled immediately.

5 Password Managing

According to our research survey, we can recognize that majority will not remember passwords due to several reasons. Using multiple different passwords for various digital accounts, character length, and complexity of it are some examples. Still, the main reason for forgetting passwords frequently is, people do not want to remember passwords at all. When it comes to passwords, people have an opinion that they bother them; so they act irresponsibly and carelessly when interacting with passwords. They create a digital account with a new strong password then totally forget about it on the next day onward.

The majority of our society tries to skip memorizing passwords and use other methods like writing down on book/paper, save as a digital file, auto-saving on web browsers, and using password managers. Fig. 5 shows methods of saving computer passwords used by the survey participants. Writing down authentication credentials on a piece of paper is the right solution rather than forgetting them on the next day or next week. Still, if someone could reach that piece of paper or lose it, it could expose and do much more harm to them someone's digital privacy. The same theory applies to those who save credentials on electronic devices as a clear text file and auto save on the popular web browsers. Encrypting and hashing methods could also be introduced with password manager software, which has more security and best option for the people who forget about their passwords frequently and hard to manage them.

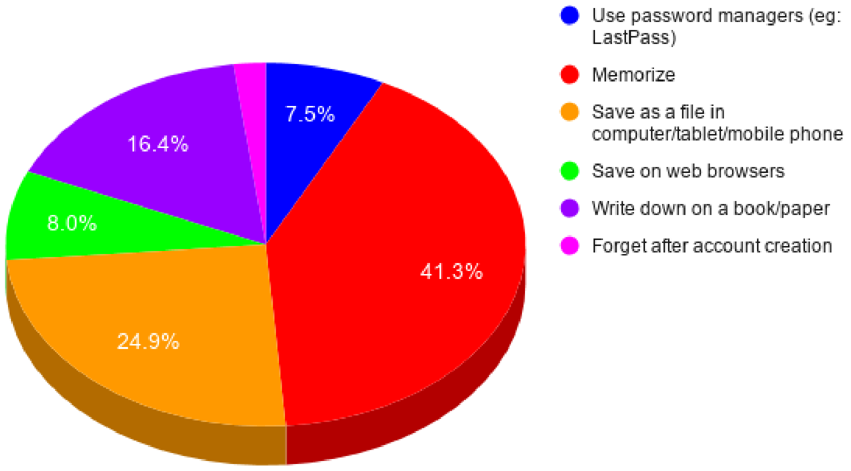

Fig. 5. Password saving methods

Another menacing thing that can be seen from our society is, using the same password for multiple accounts, and few use the same single password for all for their digital accounts for the sake of easiness of memorizing. But what they do not really understand is, if that particular password has got leaked, all of their digital accounts or some of them could be exposed, and that leads to potential security threats to their digital security and privacy. Since we cannot expect the same high level of security from every information system, it is the best practice to use different passwords for different digital accounts and update them regularly. A recent survey found that a quarter of our society had never changed passwords since the created date.

6 Additional Features

With the development of technology and issues with traditional passwords, now we are tending to use multiple biometrics to make an authentication instead of using traditional passwords such as fingerprint scanning, face recognition, voice identification, etc. Fig. 6 shows the majority of the survey participants preferred to use biometric authentication over traditional passwords. The main advantage of using biometric authentication over traditional password authentication is users of the information system do not have to memorize. They just have to present their biometric measures and gain access. Biometric also eliminates the time wastage of incorrect password attempting and recovering attempts, which helps increase the efficiency in the working environment.

This advanced technical feature is secure and very reliable since a person's biometric measures represent exactly that particular user's identity. But biometrics is still hackable, and when they do, it may have more significant consequences than we ever thought. Since a biometric reveals part of a user's true identity, if stolen, it can be used to falsify legal documents, passports, or criminal records, which can do more damage than a stolen credit card number. Once a hacker has a picture of someone's ear, eye, or finger, they can quickly gain access to their accounts.

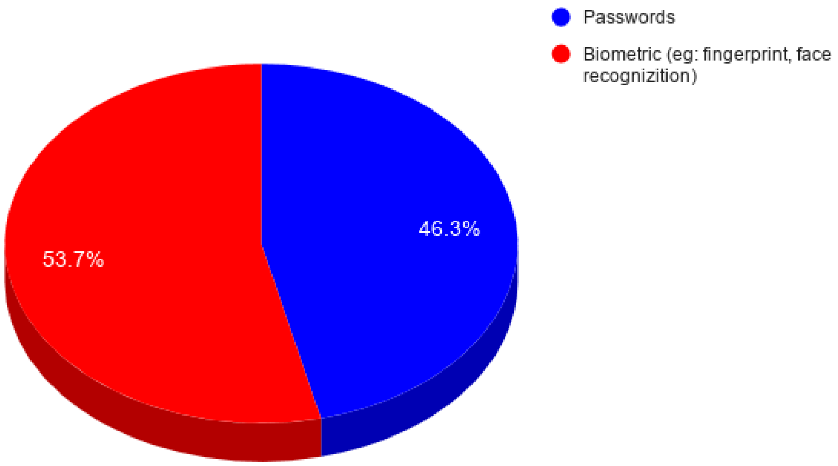

Fig. 6. Choice between biometric and password

Productive usage of biometric authentication can be seen in a lot of production environments such as educational institutes, administrational institutes, health care institutes, law enforcement units, etc. As an example, instead of manual signing sheets to record attendance of employees, fingerprint scanners are now implemented, which caused to increase productivity in both government and private sectors. Every driving license and national identity card are now issuing with respective person's biometrics. Biometric is very likely to be used as authentication mode by the majority of our society. At the same time, a significant amount tries to avoid it because of the fear of new technology and ethical questions that our traditional community is raising upon the true identity being given to the unknown.

Multi-factor authentication (MFA)is a way to authenticate to a particular information system using multiple pieces of evidence along with a password rather than relying only on passwords. Two-factor authentication (2FA) uses one different piece of evidence (factor) and a password to authenticate. One-Time-Pass code (OTP) are most likely to be used in many information systems as the factor. ATM card is the best example for 2FA as the ATM card and PIN are the two different factors that authenticate one another. 2FA can reduce the possibility a digital account is being hacked or cracked. People who seek more security for their digital accounts tend to use more than two pieces of evidence(factors) that combine a traditional password, an OTP, and a biometric to authentic. MFA secured digital accounts are very unlikely to be hacked or cracked.

As a community, all the banking and financial service providers in Sri Lanka have taken this matter very seriously and started using 2FA for most of their services like registrations, e-banking, online transactions, credit/debit card payments [5]. That is an optimistic move taken by the banking sector to bring our general public forward to the global trend with better security. Still, many other institutes are not tending to use any MFA system to secure both their information systems and user accounts. The most shocking thing is that most of our general public does not want to be bothered using 2FA or MFA, even if some popular social media platforms and email services provided the MFA. Example: - 2FA feature of both Google and Face book when logging from a new device is neglected by most of the Sri Lankans.

7 Social engineering

The weakest link of the security chain of an information system is human. It does not matter how strict a security system is; how strong the user passwords are; how advanced the technology is being used if the users could be easily manipulated to give up their credentials to the outside world [6]. Social engineering is nothing but the art of manipulating people to give up their confidential information. Phishing and Trojan attacks are the famous social engineering movements taken by hackers to crack the information systems or hack digital accounts. Fig. 7 represents the knowledge about social engineering and prevention methods of survey participants.

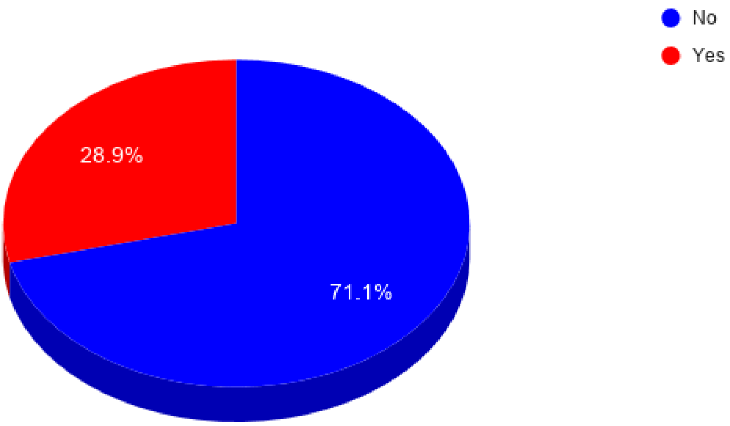

Fig. 7. Knowledge about social engineering

In 2019, Sri Lanka faced a series of powerful cyber-attacks on at least ten domestic websites with .lk and .com public domains, including Sri Lankan Kuwait Embassy Official Website [7]. Cyber-attack was recorded as a phishing attempt to gain access to the systems by spotting opportunistic security vulnerability. Unlike the USA, China, we do not face a lot of cyber-attacks frequently. Yet, we can notice many intrusions happen to social media accounts and email accounts through social engineering attempts. Through the survey results, 71% of society has no idea about social engineering. Since Sri Lanka is a low computer literacy country, our internet users can easily manipulate their sensitive information and credentials without giving much effort to cybercriminals.

8 Conclusion

According to our research, a moderate amount of Sri Lankan people has adequate knowledge regarding digital security and privacy. They start to make a lot of mistakes at the very beginning of creating a computer password. Those mistakes lead them to more significant mistakes, such as sharing their passwords, which causes more trouble and consequences to their digital security. Our country has around 33% internet users from its population with 27.5% computer literacy. The majority of our country's internet users neglect the importance of digital accounts' security and act in a manner that lacks a proper sense of responsibility. These behaviors have been able to make a considerable impact on our community. So to make this right, our society is needed to be well informed about digital security measures and how to secure themselves on the internet. Different types of solutions must be presented for different groups of people that fulfill their requirements and well-being in their digital security. Our society should be convinced to use strong passwords with full confidentiality and to move on to new trends like MFA. Password manager software can be introduced to manage their passwords and authentication processes for people who think that passwords are bothering them. Biometric authentication is also a better solution for a low computer literacy community like us to stay safe in the digital world.

9 References

[1]Robert Morris and Ken Thompson, Password Security: A Case History, Bell Laboratories, 1-2, 1979

[2] internetworldstats.com, Internet Usage in Asia, 2020

[3] SLCERT|CC, Youth survey on Social Media Security and Privacy, SLCERT|CC, 11-12, 2017

[4]Gongzhu Hu, On Password Strength: A Survey and Analysis, Central Michigan University, 2018

[5] Kasun Wijeratne, Expansion of internet banking – Overcoming the barriers, DFCC Bank PLC, 4-6, 2015

[6] Breda F., Barbosa H., Moraise T., Social Engineering and Cyber Security, University of Porto, 2017

[7] dailynews.lk, Cyber-attack on several websites including Kuwait Embassy, 2019