Password Theft Protection

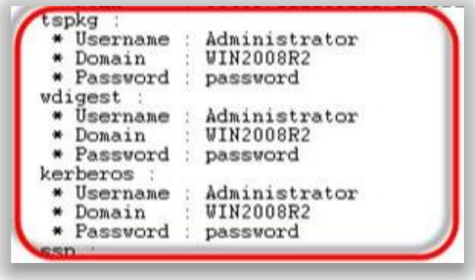
Vishnu Menon
Keraleeya Samajam (Regd.) Dombivli's Model College

Abstract:- In today's world password has been the most important method to secure ourselves from fraud and other scams. Even though some of the people does not use password to secure the device or files. Some of them use default passwords like "abc$1234" or "admin", etc which find it easy to remember. The use of strong password with minimum 16 characters is advised. We will see how password were used, how they are used currently, what are the threats of weak password usage, how to avoid those risks and to implement new methods of password policy.

Keywords:- *Password, Password Attack Techniques, Attack Tools Used, One-Time Password (OTP) and Biometrics.*

I. INTRODUCTION

In 1961, the first computer password was developed at Massachusetts Institute of Technology for using CTSS (Compatible Time-Sharing System). CTSS is used to accommodate multiple users at once by same core processor powering separate consoles. Earlier passwords were stored in the system in a plain-text format with no security measures.



```
tspkg :
  * Username : Administrator
  * Domain   : WIN2008R2
  * Password : password
wdigest :
  * Username : Administrator
  * Domain   : WIN2008R2
  * Password : password
kerberos :
  * Username : Administrator
  * Domain   : WIN2008R2
  * Password : password
ssp :
```

Fig 1

This gave the attacker full access to the computer. Nowadays various methods have been implemented to store the password in an encrypted format to make the attacker difficult to crack the password or steal it. But there are ways introduced by hackers to crack the encrypted password. We will look into these cracking and other techniques that hackers or fraudster adopt to compromise the password.

II. LITERATURE REVIEW

The use of password was introduced in 1961 for the computer for using CTSS (Compatible Time-Sharing System). In early days, people were not aware of the risk that was caused due to password stealth as they did not understand the importance of access rights they had. As a result of this the password they used were short and easy to guess which helped the attacker gain unauthorized access to the system or files. Often, they used to save their password in a notepad files or sticky notes or often write somewhere in the notebook or paper which was visible to them also to anyone who take a glimpse of the notebook. Nowadays, people are aware of not storing the password or their credentials in notepad or sticky notes or in the notebook. But there are some other security threats that the users face in today's world in which they tend to share their credentials unknowingly which is possible by the methods such as scam or fraud calls/emails.

III. METHODS AND MATERIALS

During the research, we used the survey method to find out whether people or the users of any organization adopted the appropriate password policy. We have conducted the research by questionnaire using Google Form. After conducting the survey, we found out that 53% of the users does not follow proper password policy and hence they can be an easy target of the attacker. Some of them have adopted the proper password policy.

IV. PASSWORD ATTACK TECHNIQUES

There are several ways to compromise a password of the user. The passwords can be stolen or sniffed from the network by various ways. The attack techniques are given below: -

- **Social Engineering**: - This attack was introduced during the time of Trojan Horse. It is a technique to trick the people or user to reveal their password during communication they feel as legible or normal. It is the most common used techniques during spam calls or fraudulent calls from banks and other areas. People often fall prey to this kind of attacks. Most Trending Social Engineering Attacks are as follows: -

- Pretexting
- Tailgating
- Quid Pro Quo

Fig 2

- **Shoulder Surfing**: **-** These attacks were adopted in the early 1980s to steal calling card digits details to make long distance calls and sell them in markets for the cheaper price. These kinds of attacks are being used by attackers after gaining access inside the organization. They gain physical access into the organization by tailgating (following a legitimate user) by pretending to have a deep conversation on the phone. After gaining access the attacker snoop over the shoulders of the user or staff to glimpse the password being entered by them. These attacks are rarely adopted by the attackers as the physical security has now being tightly handled by the organization.
- **Brute Force Attack**: **-** This attack is another commonly used password attack techniques in which the attacker or hacker tries all possible combinations of alphabets or numbers to get the user's password. The attack becomes easy for attackers after successful social engineering attack since they get the idea of the how the user or staff must have set the password. Mostly the user keeps simple easy-to-remember password for their convenience such as name with their birthday or year of birth or the name of their pets. This makes attackers easy to compromise their account password.
- **Key Logger Attack: -** The first keylogger that came out in 1970 is hardware keylogger. The Hardware Keylogger was installed in typewriters. Keyloggers can be hardware or software keyloggers. The software keylogger was found embedded in the most popular computer game mod "Grand Theft Auto V" in the year 2015. This records all the keystrokes that the user enters. The attackers make use of the keyloggers to record the keystrokes when the user enters the username and password or some other sensitive information in particular sites, for example, bank sites, etc. These software keyloggers comes embedded in most of the cracked version of the softwares which the user downloads from untrusted websites for their benefits of not buying the softwares legally from the trusted sites. Hardware keyloggers need physical access to the system to insert pd or rubber ducky USB as hardware keyloggers. Hence hardware keyloggers is an outdated method.

V. TOOLS USED FOR PASSWORD ATTACK & CRACKING

A. Tools Used for Stealing the Password: -

- **Social Engineering Toolkit (SET): -** The SET is used by attacker mostly to create a phishing website of the legitimate website to gather username and password or some other confidential information like payment details.
- **Wireshark: -** It is used by attacker to sniff the username and password that the user enters while connected to the network. The attacker gains access to the network that the user is connected in or creates a Fake Access Point while keeping it open for the user to get the user easily connected to the attacker's network for further malicious actions.
- **Cain and Abel: -** The attacker make use of this software to steal the credentials from the users. It is also used to perform Man-In-The-Middle Attack which can lead to password theft**.**

B. Tools Used for Cracking Password: -

Even though the attacker successfully sniffed the password, it might be of no use as it may encrypted using cryptographic algorithm. The attacker found some ways to crack those encryptions. Below are those methods used by attackers: -

- **Hashcat**: -It is the world's fastest recovery tool using for cracking the encrypted password. This software decrypts almost all the encryption methods like MD5, AES, etc. It is an open source and hence mostly adopted by the attackers.
- **John the Ripper**: **-** It is a password cracking tool that is used to decrypt hash value into the plain text from the wordlist given at the time of cracking.
- **Cain**: **-** It is a password cracking tool along with password stealing. It needs to be provided the hash value and the type of encryption used for encrypting the password and also needs to provide the necessary way of attack to be performed like dictionary or brute force attack.

VI. METHODS TO PROTECT PASSWORD THEFT AND CRACKING

As per the survey and research conducted, it has been observed that some of the user tends to use password which is short and easy to remember, they tend to write somewhere in the notepad or sticky notes in the computer or in notebooks which is not a good security practices adopted by the people. According of the research conducted, some of the users and people tend to use the same password everywhere they require to sign-in due to which the other websites or devices using the same password gets compromised. There are also incidents where the long complex passwords also get leaked after it has been stolen. Some of the security measures needs to be implemented as a mandatory option for the users to adopt to maintain security of their devices and files. The security measures are as follows: -

- *For Users: -*

- Don't keep blind faith on the people which is on other sides of the phone call asking for personal details.
- Always check for the URL whether it is spelled correctly and also whether it starts with https://
- Bank never asks for the internet banking credential details for security reasons.
- Always adopt the practice of using 16 characters for password which consist of Capital Letters, small letters, numbers and special characters.
- Adopt the practise of renewing the password weekly or monthly and use different password at the time of renewal.
- Avoid using the same passwords everywhere for your convenience.

- Strictly adopt the policy of 2Factor-Authentication which consist of Password and OTP or Password and Biometrics.
- Never share your password with your family or colleagues or friends.

➢ *For Security and Developer Personnel: -*

- Strictly implement 2Factor-Authentication.
- Strictly warn the user to change their password weekly or monthly.
- Strictly implement password length to be more than 12 characters with upper- and lower-case letters, numbers, special characters.
- Strictly implement session timeout when the session is idle.
- If session timeout is implemented, reduce the idle time of the website.
- Strictly make use of POST () method instead of GET () method.
- Adopt best encryption standard while transporting username and password through the channel.

VII. DATA AND RESULTS

According to the data that we have collected from the survey we found out that 53% of the user does not take the password policy, seriously. The rest of the people follows proper implementation of password policy. **Fig 3** shows the number of people who are from IT and non-IT department. 67.3% are from IT department. 32.7% are from non-IT department. **Fig 4** shows the number of the people, whether they set password or leave the device and files as it is. It has been observed that 95.9% of the people surveyed make use of the password. **Fig 5** gives an idea of the importance shown by the people to set password for their devices and files. It has been found that 98% of the people find it important to have their devices and files password-protected. **Fig 6** shows the kind of password they set to protect themselves from attack. It is found that 59.2% of the people make use of hard-to-guess and complex password. **Fig 7** give the percentage of the people who use the password which has less than 10 characters. It has been found out that 44.9% of the people use password that is less than 10 characters. **Fig 8** shows the number of people who uses alphanumeric characters for the password. It has been found that 8.2% and 6.1% of the people uses only alphabets and numbers respectively while creating the password for them. **Fig 9** indicates how many of the people are aware of the password theft techniques. 55.1% of the people are aware of how the password theft take place. **Fig 10** gives an idea on how often the users or people change their password once set. It has been recorded that 10.2% people doesn't change their password once it has been set. 28.6% of the people change their password occasionally. **Fig 11** gives the percentage of the people on their password memorizing behaviour. It has been found that 26.5% of the people surveyed, remembers their password by noting down somewhere. **Fig 12** gives an idea of the people whether they use the same password everywhere wherever they require to sign-in which is not a good security policy as only one password can compromise every other devices and files or website with the same password. 38.8% of the people adopts this weak security policy. **Fig 13** gives us an idea of how many percentages of the people takes 2Factor-Authentication seriously. It has been found out that 22.4% of the people doesn't adopt 2Factor-Authentication. 57.1% of the people make use of 2Factor-Authentication in some of the applications and devices. In **Fig 14,** we asked for the opinion on what will they prefer for 2Factor-Authentication. 55.1% of the people voted for Password and OTP as 2Factor and the rest 44.9% voted for Password and Biometrics. **Fig 15** shows the opinion of the user or people if new password policy has to be implemented i.e. opinion if 3Factor is to be implemented. 89.8% of the people agreed to have 3Factor-Authentication for a more stronger password security policy.

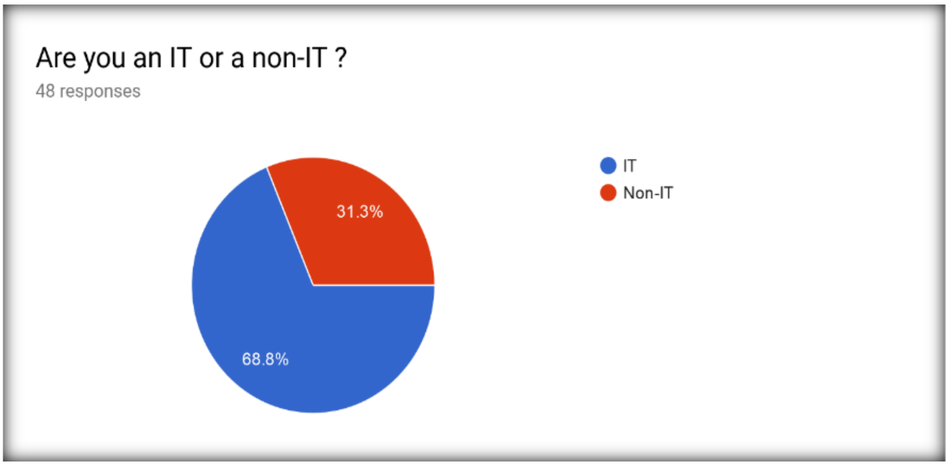


Fig 3

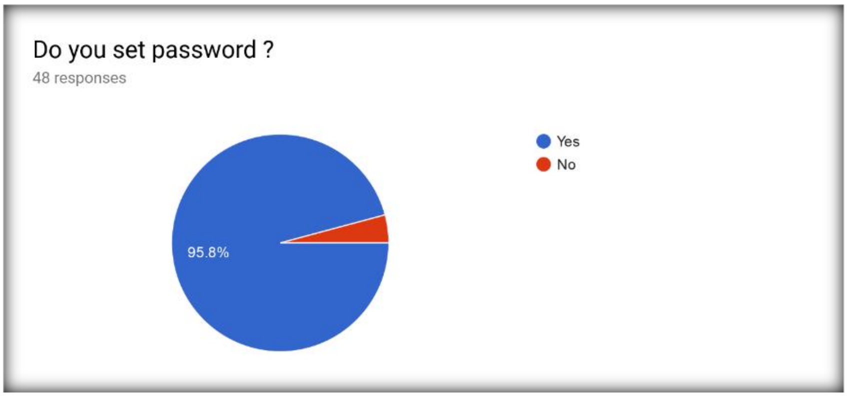


Fig 4

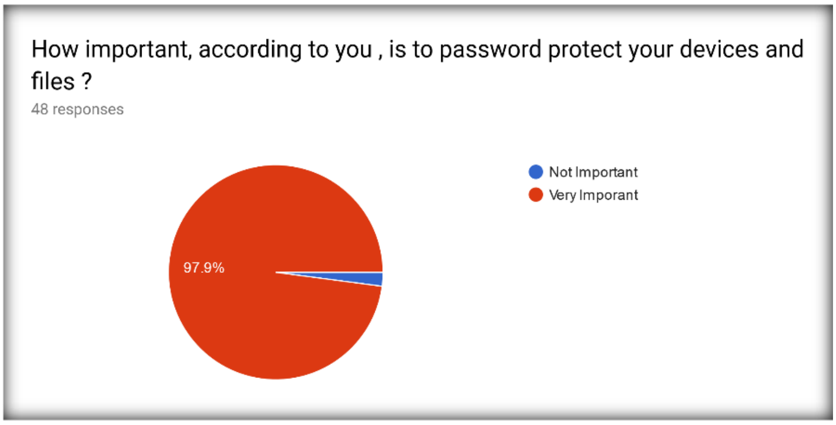


Fig 5

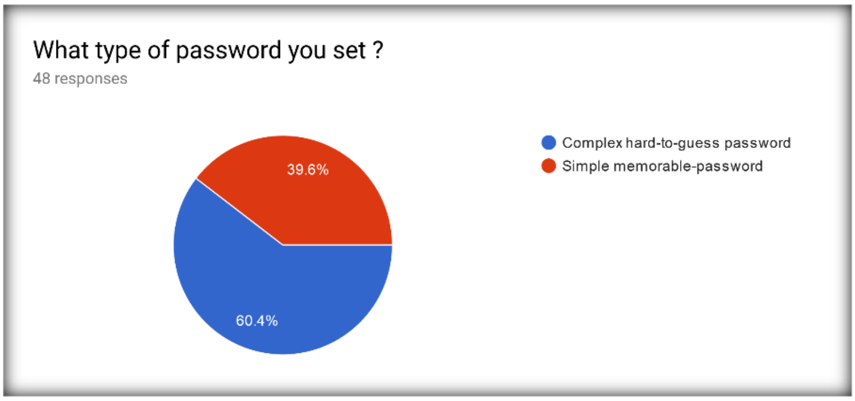


Fig 6

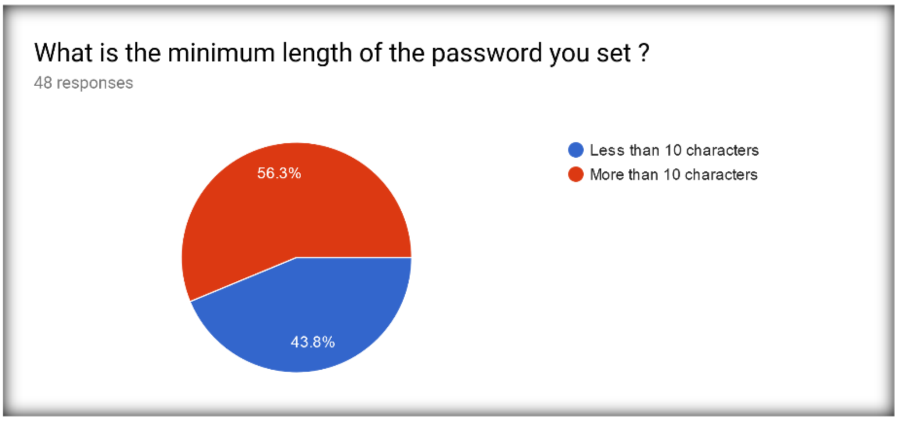


Fig 7

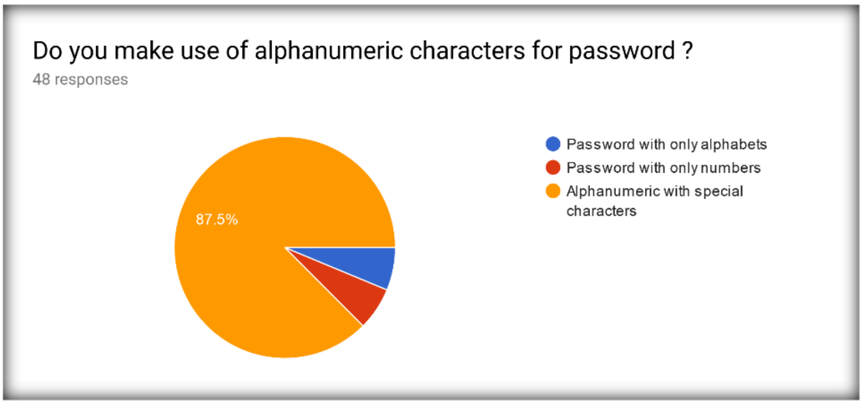


Fig 8

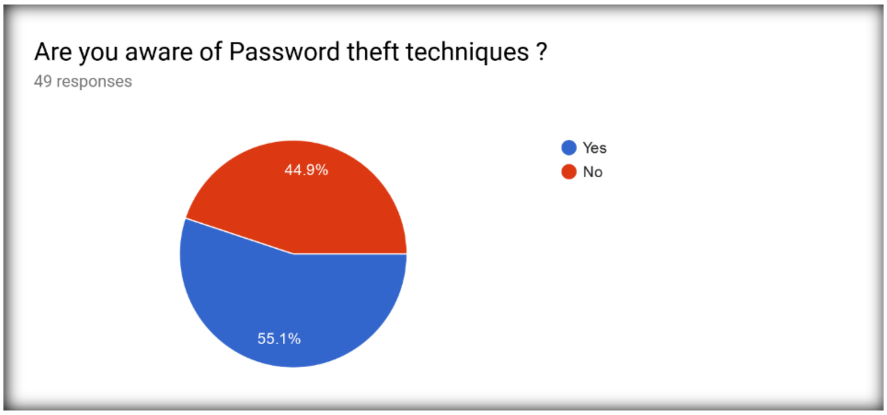


Fig 9

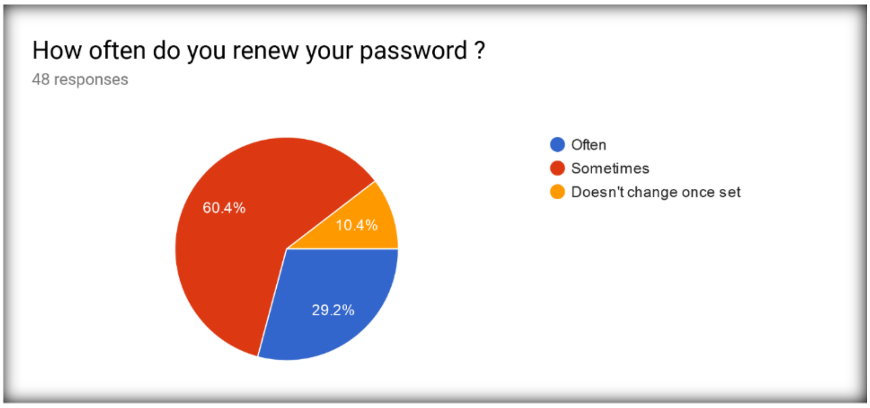


Fig 10

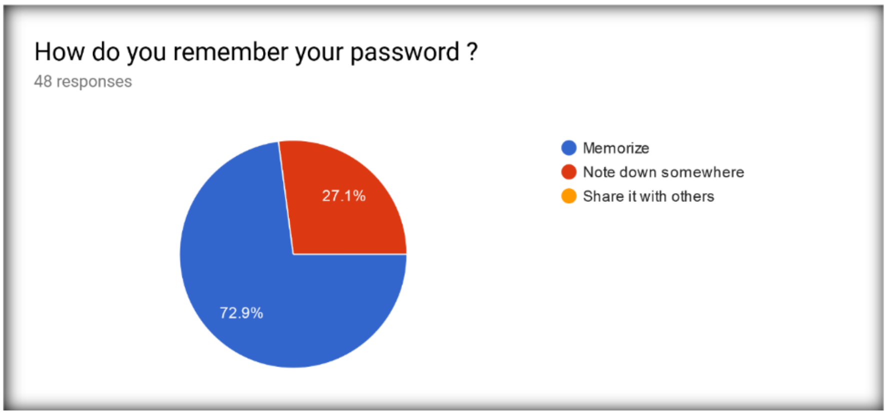
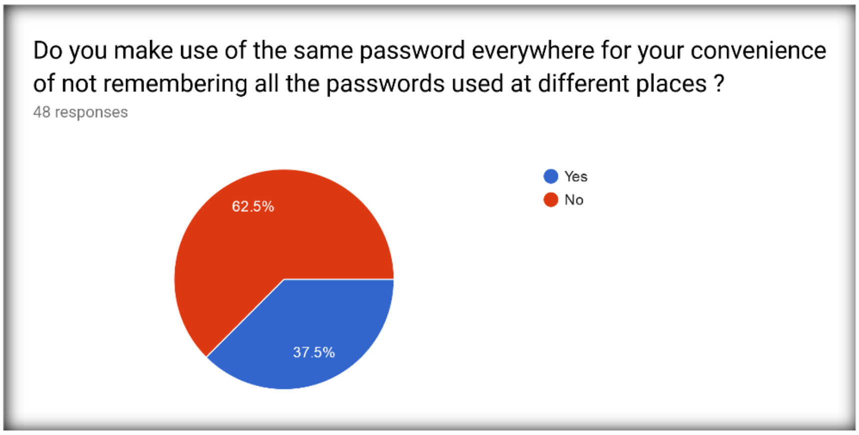


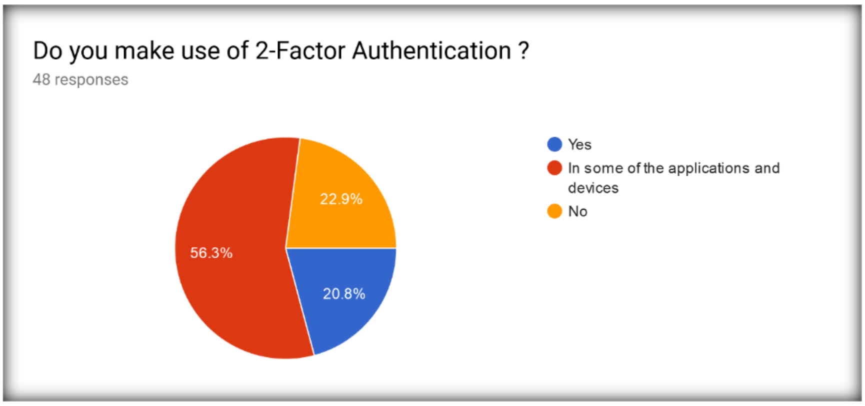
Fig 11



Do you make use of the same password everywhere for your convenience of not remembering all the passwords used at different places ?

48 responses

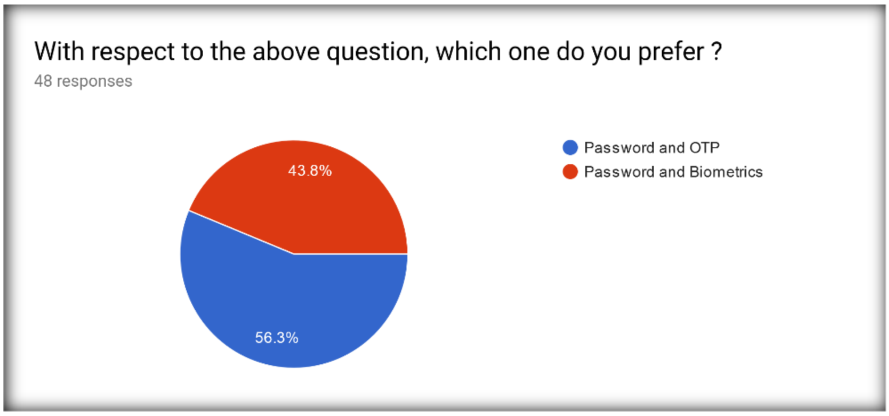
Fig 12



Do you make use of 2-Factor Authentication ?

48 responses

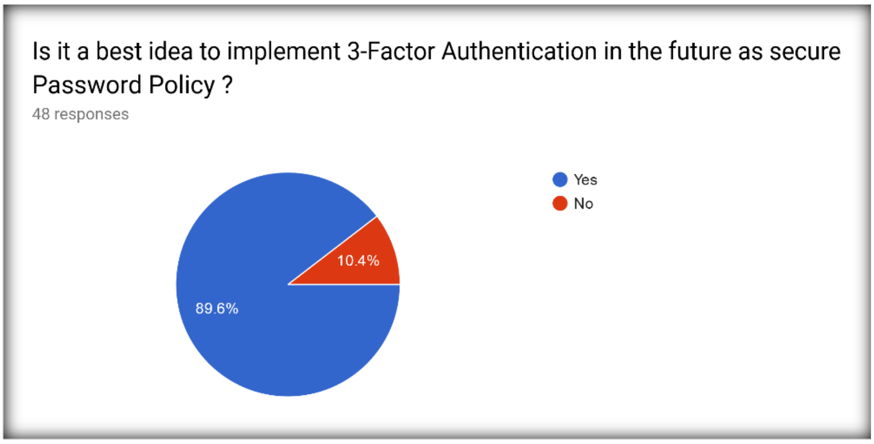
Fig 13



With respect to the above question, which one do you prefer ?

48 responses

Fig 14



Is it a best idea to implement 3-Factor Authentication in the future as secure Password Policy ?

48 responses

Fig 15

VIII. FUTURE SCOPE

The password alone cannot improve the security of the user’s confidential data or the device itself. It will add more security to the user’s data if it is used with OTP (One Time Password) as a 2Factor-Authentication feature and it must be strictly used rather than optional case to use it. We can implement new security policy if we adopt one more authentication factor i.e. Biometrics along with Password and OTP. Thus, implementing 3Factor-Authentication will make the attacker very difficult to compromise the user data even if the password has been compromised as the rest of the two will not be hackable or compromised to a greater extent. We can adopt a 3Factor in future once the 2Factor becomes the base security the user adopts.

IX. CONCLUSION

In this section, we have observed the password pattern used by the users, their weakness of revealing password to the fraudster by blindly believing in their words. Almost all the attacks can be reduced to an extent but the art of social engineering still remains the most successful form of attack as it is purely based on tricking people to believe in the words of the attackers. It is highly advisable to use 2Factor-Authentication for more security on your device and files. The 3Factor-Authentication can be of great idea in the future which can then become nearly impossible for the attackers to compromise the account or data with only password.

REFERENCES

[1]. https://hashcat.net/hashcat/
[2]. https://authanvil.com/blog/3-types-of-password-security-attacks-and-how-to-avoid-them
[3]. https://www.onelogin.com/learn/6-types-password-attacks
[4]. CEH v10 Guide Book