Attitude Survey - Final Report

Attitude Towards Passwords

Authors:

Philomina O. Ejegi Ede

Melat Getachew

Tables of Contents

1. Introduction 3
1.1. Background 3
1.2. Aim 3
1.3. Method 3
2. Hypothesis 4
3. Empirical Findings..... 5
4. Results 7
4.1. Response analysis 7
5. Analysis 11
6. Discussion 12
7. Conclusion 13

1. Introduction

The report was to investigate people's attitudes towards password preferences and password management.

1.1. Background

From the survey conducted, the purpose was to know more about people's attitudes when formulating passwords. By asking the respondents what type of authentication technique they mostly use, length of passwords, how they formulate their passwords, how often they change their passwords, and if they re-use passwords for different accounts, we validated the assumption that passwords are one of the most widespread and well-known method of authentication, with little or no idea that there could be vulnerabilities with weakness and improper management.

1.2. Aim

The aim of this report is to analyze with the use of a survey, people's attitudes towards password preferences and password management.

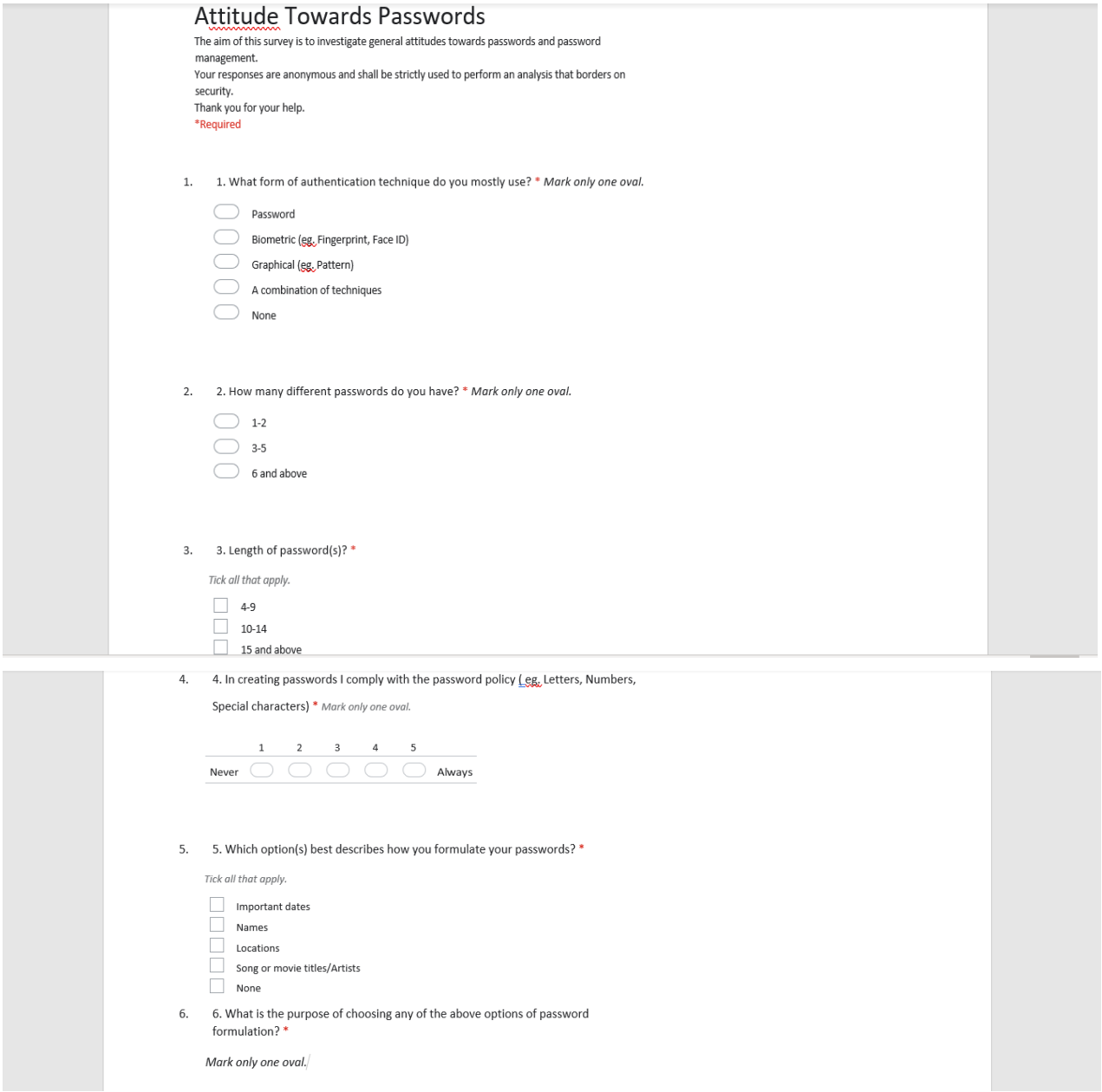
1.3. Method

The survey was conducted using Google docs survey tool and also was published on Whatsapp, Facebook, and Instagram to get as many respondents as possible.
The survey questions can be found in the "Empirical Findings" section.

2. Hypothesis

From this survey, the expected results are that there will be some differences in attitudes towards password preferences and password management. Most users tend to use weak passwords or include personal information in their passwords for different reasons and most passwords are chosen within a small portion of the entire password space, leaving them vulnerable to brute force or dictionary attacks.

3. Empirical Findings



Attitude Towards Passwords

The aim of this survey is to investigate general attitudes towards passwords and password management.
Your responses are anonymous and shall be strictly used to perform an analysis that borders on security.
Thank you for your help.
*Required

1. 1. What form of authentication technique do you mostly use? * *Mark only one oval.*
   - Password
   - Biometric (eg. Fingerprint, Face ID)
   - Graphical (eg. Pattern)
   - A combination of techniques
   - None
2. 2. How many different passwords do you have? * *Mark only one oval.*
   - 1-2
   - 3-5
   - 6 and above
3. 3. Length of password(s)? *

   Tick all that apply.
   - 4-9
   - 10-14
   - 15 and above
4. 4. In creating passwords I comply with the password policy (eg. Letters, Numbers, Special characters) * *Mark only one oval.*

	1	2	3	4	5	
Never						Always

5. 5. Which option(s) best describes how you formulate your passwords? *

   Tick all that apply.
   - Important dates
   - Names
   - Locations
   - Song or movie titles/Artists
   - None
6. 6. What is the purpose of choosing any of the above options of password formulation? *

   Mark only one oval.

- Easy to remember
- Easy to formulate
- To make it difficult for anyone to guess
- All of the above
- None

7. 7. Do you re-use passwords for different accounts? *

Mark only one oval.

	1	2	3	4	5	
Never, I have unique passwords for different accounts						Always, I use the same password for all my accounts

8. 8. When necessary I disclose/share my password with someone. *

Mark only one oval.

	1	2	3	4	5	
Disagree						Agree

9. 9. How often do you change your password(s)? * *Mark only one oval.*

- 3-6 month
- Yearly
- When I forget my password(password reset)
- Never

10. 10. Do you save your passwords on your devices? *

Mark only one oval.

	1	2	3	4	5	
Never						Always

11. 11. Do you feel that password policies make you more secure? *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree						Strongly agree

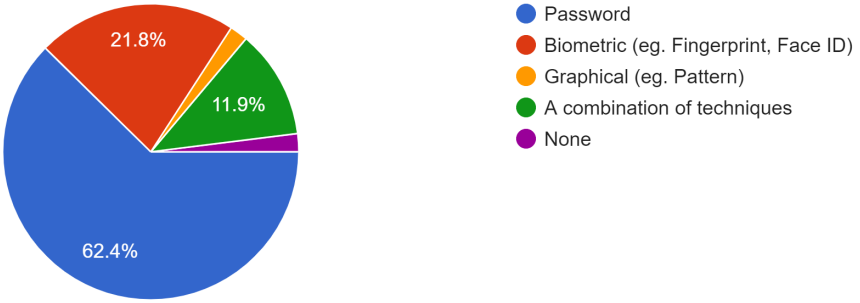
4. Results

This survey contains 11 questions. The results are introduced below:

4.1 Response analysis

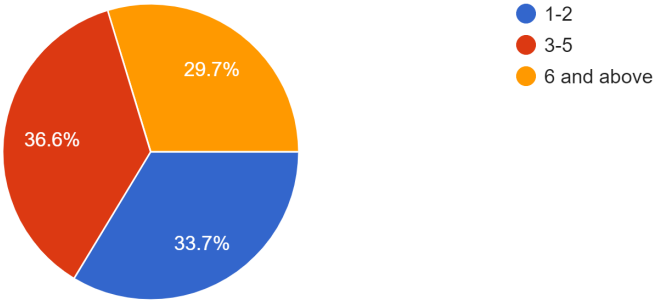
1. What form of authentication technique do you mostly use?

101 responses



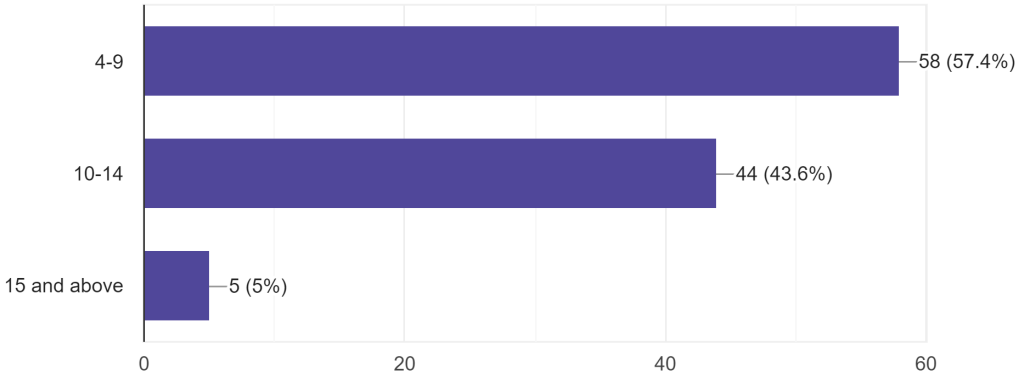
2. How many different passwords do you have?

101 responses



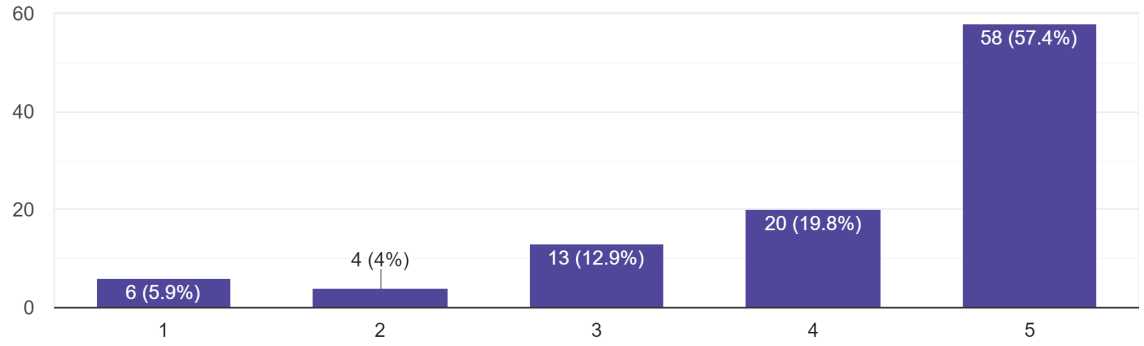
3. Length of password(s)?

101 responses



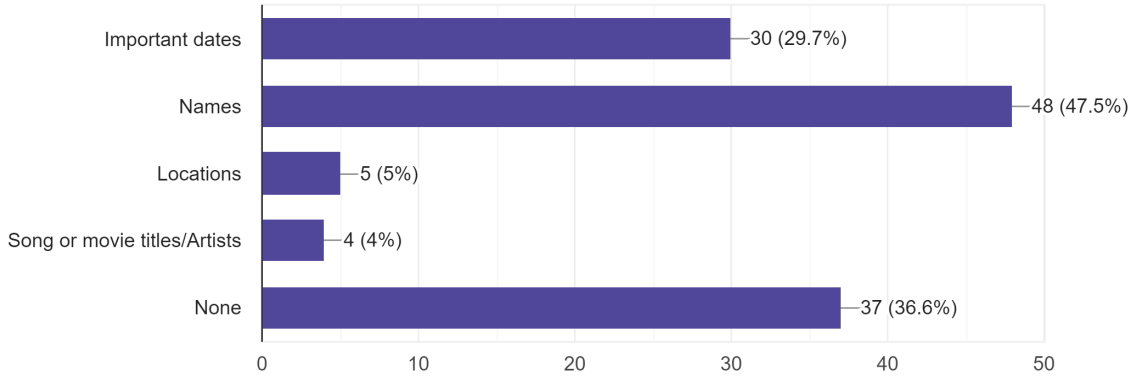
4. In creating passwords I comply with the password policy (eg. Letters, Numbers, Special characters)

101 responses



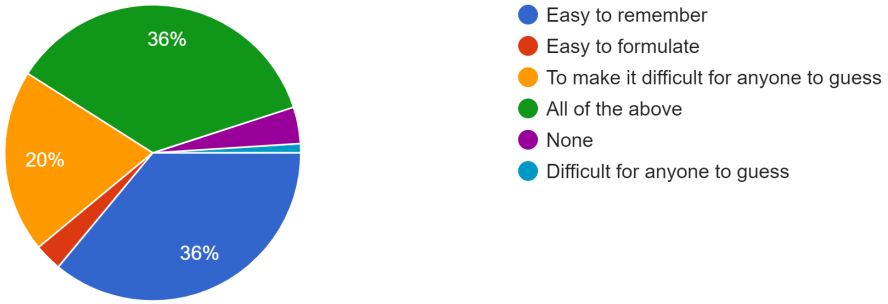
5. Which option(s) best describes how you formulate your passwords?

101 responses



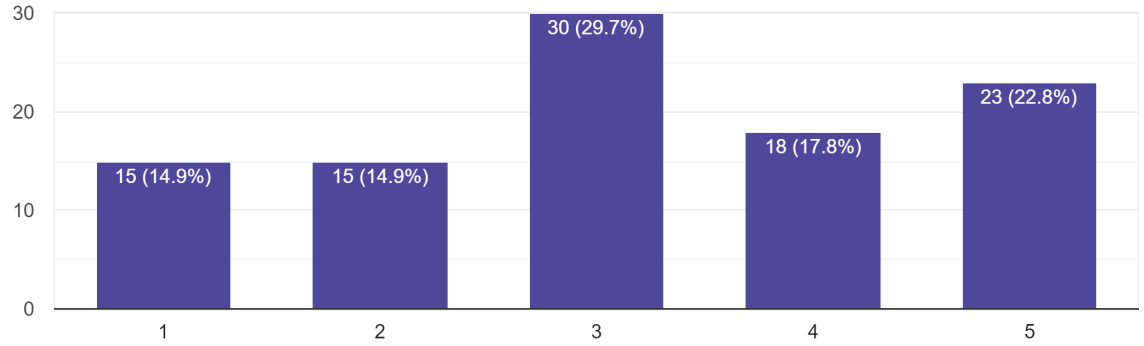
6. What is the purpose of choosing any of the above options of password formulation?

100 responses



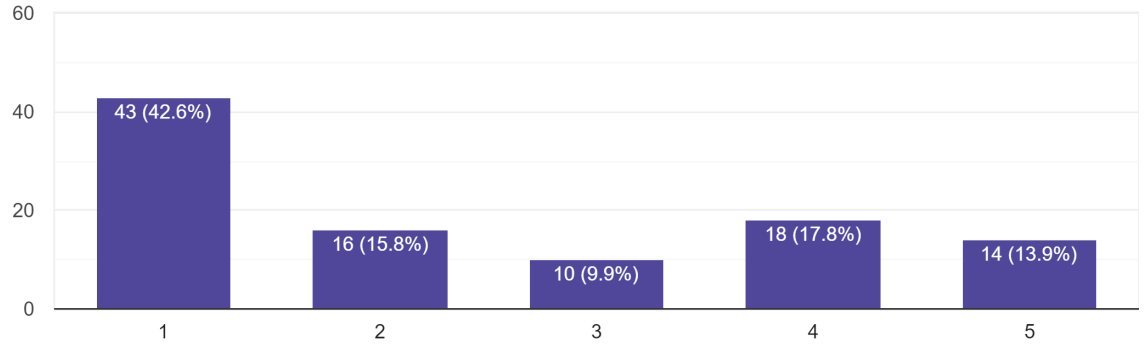
7. Do you re-use passwords for different accounts?

101 responses



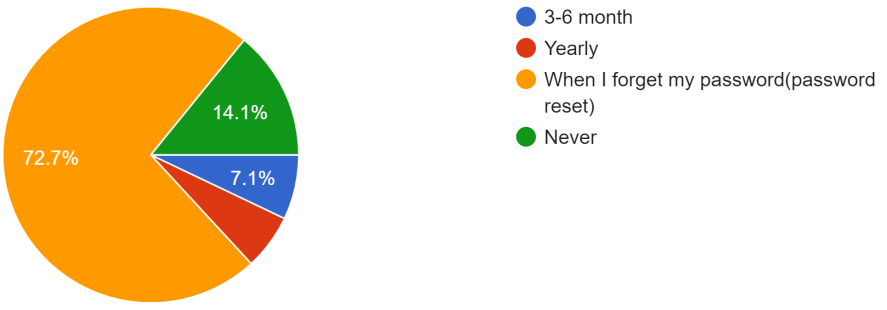
8. When necessary I disclose/share my password with someone.

101 responses



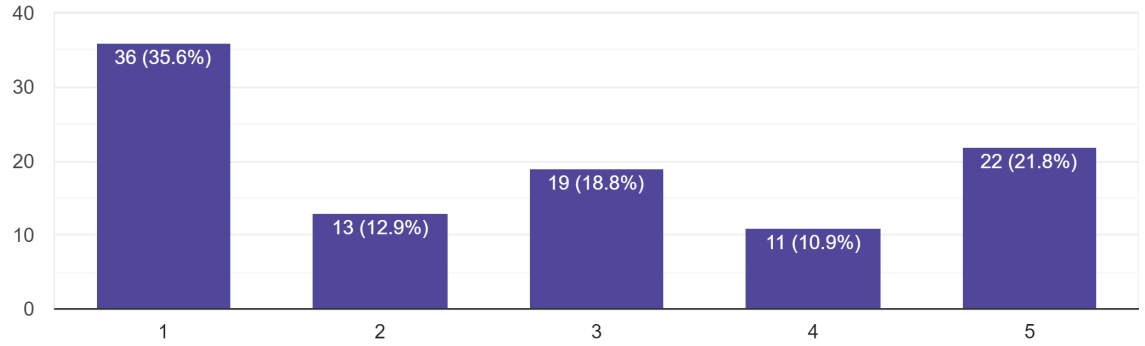
9. How often do you change your password(s)?

99 responses



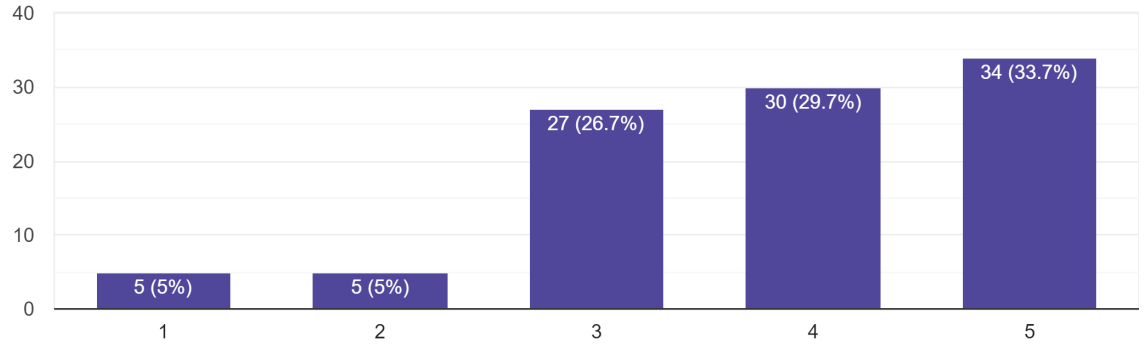
10. Do you save your passwords on your devices?

101 responses



11. Do you feel that password policies make you more secure?

101 responses



5. Analysis

101 respondents filled out the survey. From the results, 62.4% use passwords as authentication technique, 21.8% use biometric, 2% use graphical technique, and 11.9% use a combination of techniques. This is to affirm the claim that password is the most preferred and used authentication technique.

For the total number of different passwords they have, 33.7% had at most 2, 36.6% had at most 5 and 29.7% had 6 and above different passwords.

When asked the length of their password, the result shows that 57.4% had 6 to 9, 43.6% had 10 to 14 and 5% had 15 and above characters.

In compliance with password policies, 57% of the respondents strongly comply with password policies on a scale of 1 to 5. On the average, 90% of the respondents comply with password policy in general.

When asked how they formulate their passwords, results show that 47.5% include names, 29.7% include important dates, 5% include locations, 4% include songs or movie titles and 36.6% include none of the above in their password formulation. Furthermore, reasons for the choices made above reflected that 36% - “easy to remember”, 3% - “ easy to formulate”, 21% - “ to make it difficult for anyone to guess”, 36% - “all of the above”, and 4% - “none”.

Responses from the re-use of passwords on a scale of 1 to 5 show that 30% had unique passwords for different accounts and 70% of the respondents re-use their passwords for different accounts.

When asked if they agree to share their password when necessary, the result shows that 58% strongly disagreed, 9.9% agreed, and 31% strongly agreed.

When asked how often they change their passwords, 72.7% change password only when they forgot (password reset), while 7.1% every 3-6 months, 6.1% yearly, and 14.1% have never changed their password.

When asked if they save their passwords on their devices on a scale of 1 to 5, 48% strongly disagreed, 18.8% agreed, and 32% strongly agreed.

When asked if they agree that password policies make them more secure on a scale of 1 to 5, 10% strongly disagreed, 26.7% agreed, and 63% strongly agreed.

6. Discussion

As mentioned earlier, the practice of password has been in use over time till date and it is still the most preferred type of authentication technique. According to our findings, it is evident that, although password is the most widespread and well-known method of authentication, people have little or no idea that there could be vulnerabilities with weakness and improper management of passwords.

From the survey, seventy percent of the respondents have less than 5 different passwords and ninety-five percent use less than 15 characters for their passwords. These passwords are easily broken under few seconds with the latest password-cracking softwares. Furthermore, the results of this study also show that over seventy percent of the respondents indicated that for the purposes of “easy to remember” and “easy to formulate” they often formulate passwords based on their personal information such as names, important dates, location and their favorite artists/titles of songs or movies. Such password formulations can easily be guessed by family members, friends, and colleagues.

Another problem we observed in the results of this study is that seventy percent of the respondents often re-use passwords for different accounts and more than eighty percent never change their passwords unless when compelled to do so. This can lead to hackers gaining multiple access using one password which is a serious problem because the users do not have an idea that their passwords have already been compromised.

A number of good attitudes that however were noticed are that nearly sixty percent of the respondents do not share their password with someone and do not save passwords on their browsers or devices.

7. Conclusion

In the course of the report, we got to know about password manager software applications which assists in formulating complex passwords and storing them in an encrypted database to enhance password security. This is an updated information about the report which is useful for future purposes.

In conclusion, the findings of this study support the hypothesis that users display different attitudes towards password preferences and password management and that most users use weak passwords and include personal information in their passwords for different reasons. Clearly, users are less aware that these attitudes can make them vulnerable to attacks. This study recommends that users should comply strictly with password policies to enable them become more secure with using passwords as their choice of authentication technique.