CHAPTER IV

RESULTS AND DISCUSSION

4.1 INTRODUCTION

The study has three main objectives namely; to study the social engineering techniques; to study the effect of social engineering techniques on traditional and graphical password authentications and to evaluate the best type of graphical password that is secure from password guessing. This chapter discusses results from data collection; the results are classified into three parts; the first part contains the result that related to objective one, the second part contains the results that related to objective two and the third part contains the results that related to objective three.

A survey questionnaire was conducted to achieve the third objective; the results were categorized into; the first part analyses the demographic data related to the personal information such as; gender, education background and the participant's university. The second part illustrates the choice-based graphical password attempts to obtain the needed password. The third part analyses the click-based graphical password attempts to obtain the required password. The final section analyses the pattern repetition for choice-based graphical password and click-based graphical password.

4.2 RESULTS RELATED TO OBJECTIVE ONE

The first objective of the research is to study the social engineering techniques. The social engineering techniques were studied based on the literature review; seventeen techniques were defined in Chapter II. The second step is to classify the social engineering techniques.

Based on the literature review social engineering attacks can be classified into four groups depending on the exploitation of one of the weaknesses (Figure 8);

1- The first group consists of the techniques that exploiting the victim's confidence, this group contains; trusted domain, vishing (voice phishing) attack, piggybacking tactic, confidence-building, trusted e-mail source, a whaling attack, generic sender, attention-grabbing subject, guessing attack, reverse social engineering (RSE) and techie talk tactic.

2- The second group consists of techniques based on greed; it contains spear phishing and phishing attacks.

3- The third group based on the curiosity and it contains social networking sites attacks and exploiting the sex attacks.

4- The final group based on the human psychology; it contains neuro-linguistic programming (NLP) and exploiting humans' problems.

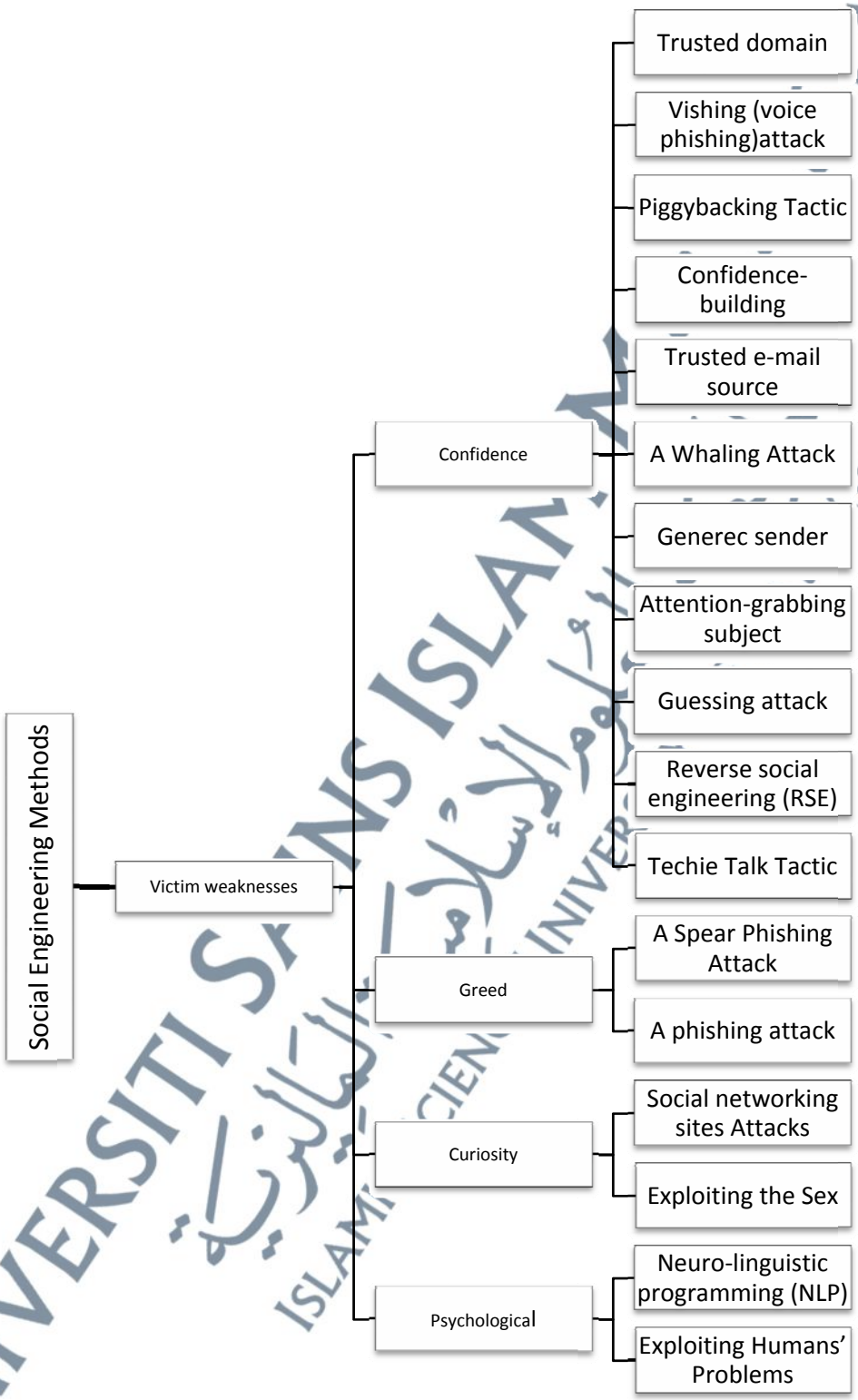

Figure 8: SEM classification

4.3 RESULTS RELATED TO OBJECTIVE TWO

The second objective of the research is to study the effect of social engineering techniques on traditional and graphical password authentications. Based on the literature review, the study summaries the social engineering attacks impact on both of the graphical passwords GP and the traditional passwords TP (Table 6) based on the literature review (Table 7).

TABLE 6: Traditional and Graphical password attacks

Social Engineering attacks	**TP**	**GP**
1-Attention-grabbing subject	√	×
2-Trusted e-mail source	√	√
3-Confidence-building	√	×
4-Trusted domain	√	×
5- Generic sender	√	×
6-Reverse social engineering	√	×
7- Piggybacking Tactic	√	×
8- Techie Talk Tactic	√	×
9- A phishing attack	√	√
10- A Spear Phishing Attack	√	√
11- A Whaling Attack	√	×
12- Vishing (voice phishing) attack	√	×
13- Social networking sites Attacks	√	×
14-Neuro-linguistic programming (NLP) Attacks	√	×
15- Exploiting the Sex	√	×
16- Exploiting humans' problems	√	×
17-Guessing attacks	√	√
√ there is an effect × there is not an effect		

TABLE 7: Graphical and Traditional password attacks references

Social Engineering attacks	**Graphical passwords**	**Traditional passwords**
1-Attention-grabbing subject	Almaula (2008) and Khan *et al.* (2011)	Roth *et al*. (2004); Tari *et al.* (2006); Backes *et al*. (2008); Laxton *et al*. (2008); *et al*. (2011); Lashkari *et al.* (2012) and Dunphy (2013)
2-Trusted e-mail source	Biddle *et al.* (2011)	Roth *et al.* (2004); Tari *et al.* (2006); Backes *et al*. (2008); Laxton *et al*. (2008); *et al.* (2011); Lashkari *et al.* (2012) and Dunphy (2013)
3-Confidence-building	Almaula (2008) and Khan *et al*. (2011)	Roth *et al*. (2004); Tari *et al.* (2006); Backes *et al*. (2008); Laxton *et al.* (2008); *et al.* (2011); Lashkari *et al*. (2012) and Dunphy (2013)
4- Piggybacking Tactic	Almaula (2008) and Khan *et al*. (2011)	Tari *et al.* (2006); Backes *et al.* (2008); Laxton *et al.* (2008); Roth *et al.* (2004); and Khan *et al.* (2011)
5- Techie Talk Tactic:	Almaula (2008) and Khan *et al*. (2011)	Tari *et al.* (2006); Backes *et al.* (2008); Laxton *et al*. (2008); Roth *et al*. (2004); and Khan *et al.* (2011)
6- A phishing attack	Mitnick & Simon (2002); Almaula (2008); Khan *et al.* (2011); Stobert *et al*. (2012) and Dunphy (2013)	Roth *et al*. (2004); Tari *et al.* (2006); Backes *et al.* (2008); Laxton *et al.* (2008); *et al*. (2011); Stobert *et al*. (2012); Lashkari *et al.* (2012) and Dunphy (2013)
7- A Spear Phishing Attack	Almaula (2008); Khan *et al.* (2011); Stobert *et al*. (2012) and Dunphy (2013)	Roth *et al.* (2004); Tari *et al.* (2006); Backes *et al.* (2008); Laxton *et al.* (2008); *et al.* (2011); Stobert *et al.* (2012) and Dunphy (2013)
8- A Whaling Attack	Almaula (2008) and Khan *et al.* (2011)	Khan *et al.* (2011); Lashkari *et al.* (2012) and Dunphy (2013)
9- Vishing (voice phishing) attack	Almaula (2008); Khan *et al.* (2011); Stobert *et al.* (2012) and Dunphy (2013)	Roth *et al.* (2004); Tari *et al.* (2006); Backes *et al.* (2008); Laxton *et al.* (2008); *et al.* (2011); Stobert *et al.* (2012); Lashkari *et al.* (2012) and Dunphy (2013)
10- Social networking sites Attacks	Almaula (2008) and Khan *et al.* (2011)	Roth *et al*. (2004); Tari *et al.* (2006); Backes *et al.* (2008); Laxton *et al.* (2008) and Khan *et al.* (2011)
11-Neuro-linguistic programming (NLP) Attacks	Almaula (2008) and Khan *et al*. (2011)	Roth *et al.* (2004); Tari *et al.* (2006); Backes *et al.* (2008); Laxton *et al*. (2008); *et al*. (2011) Lashkari *et al.* (2012) and Dunphy (2013)
12- Exploiting the Sex	Almaula (2008) and Khan *et al*. (2011)	Roth *et al.* (2004); Tari *et al.* (2006); Backes *et al.* (2008); Laxton *et al.* (2008) and Khan *et al*. (2011)
13- Guessing attacks	Almaula (2008) and Khan *et al.* (2011)	Roth *et al*. (2004); Tari *et al.* (2006); Backes *et al*. (2008); Laxton *et al*. (2008) and Khan *et al*. (2011)

4.4 RESULTS RELATED TO OBJECTIVE THREE

The third objective of the research is to evaluate the best type of graphical password that is secure. This study assesses the effect of guessing attack as a branch of social engineering attacks against the click-based graphical password and choice-based graphical password.

4.4.1 Demographic Data

The questionnaire was distributed to 50 participants. The majority of the participants are females; whereas 16 males (Figure 9). The majority of the participant are USIM students; consisting of 28 participants from Universiti Sains Islam Malaysia (USIM) and 22 participants from Universiti Kebangsaan Malaysia (UKM) (Figure 10). Thirty seven participants are undergraduate students, and 13 are postgraduate students (Figure 11).

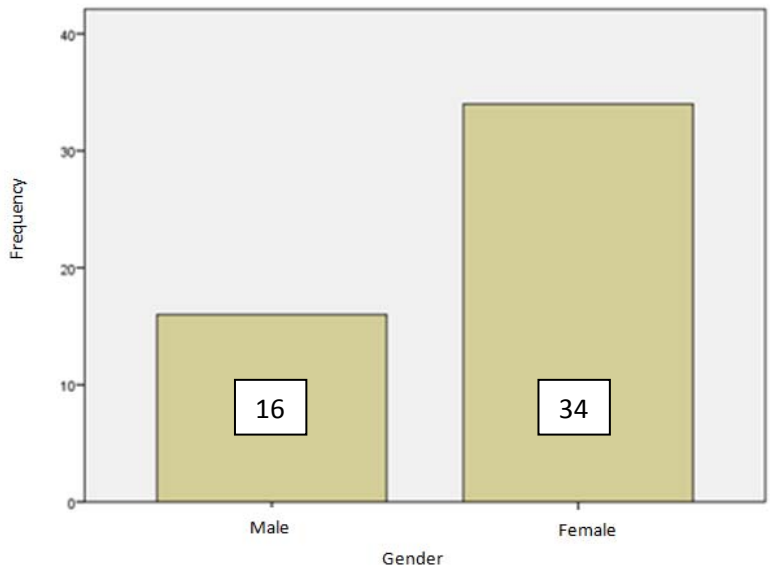

Figure 9: Participants gender

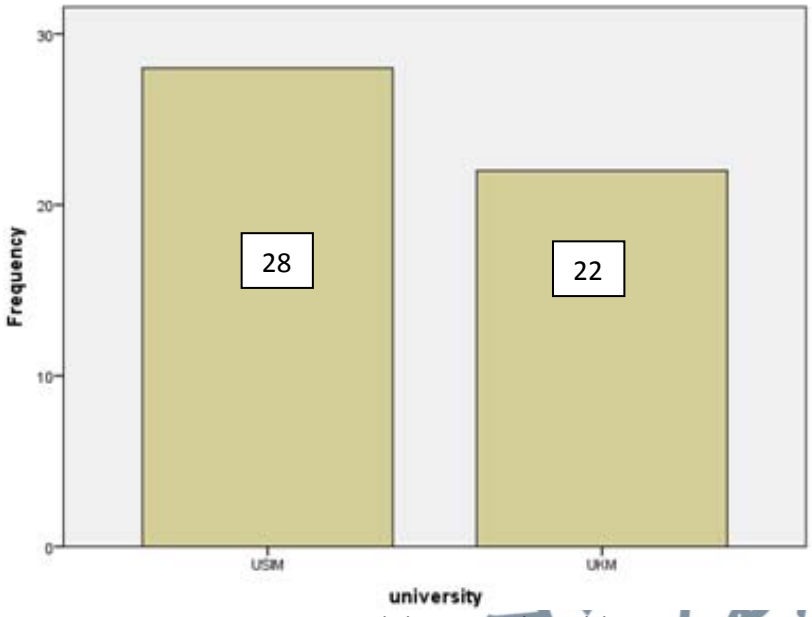

Figure 10: Participants universities

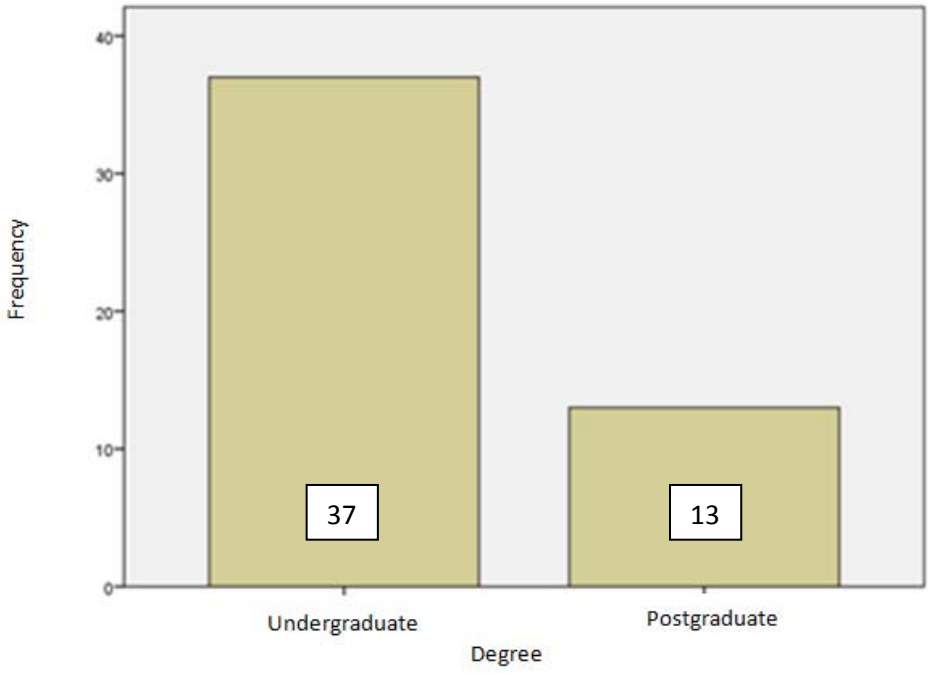

Figure 11: Students level of study

4.4.2 Choice-Based Graphical Password

The choice-based method presented nine objects. The role of the participants is to guess the choice-based graphical password, which already is determined earlier before the questionnaires were distributed. Each participant was given three attempts at choice-based method and click-based method to get the required passwords.

The required choice-based graphical password consists of five objects, namely; fish, butterfly, flower, clock and house respectively. Each object has its own symbol, so the participants have to write down the symbols for each attempt, whereas, the required password is O, J, T, S, and E for the choice-based graphical password.

1. Choice-based Graphical Password- First Attempt

By comparing the passwords that the participants were guessed in the questionnaire with the correct password; all the participants in the first attempt did not guess the required password (Table 8), whereas 50 participants have incorrect passwords. Figure 12 illustrates the repetition of the objects, that were used in the first attempt, it shows that the most objects that were used by the participants to guess the password are; the most one is S (clock), then E (house), V (coffee) and finally W (faces).

TABLE 8: Attempt one (Choice-based graphical passwords)

	Frequency	Percent	Valid Percent	Cumulative Percent
not correct	50	100.0	100.0	100.0

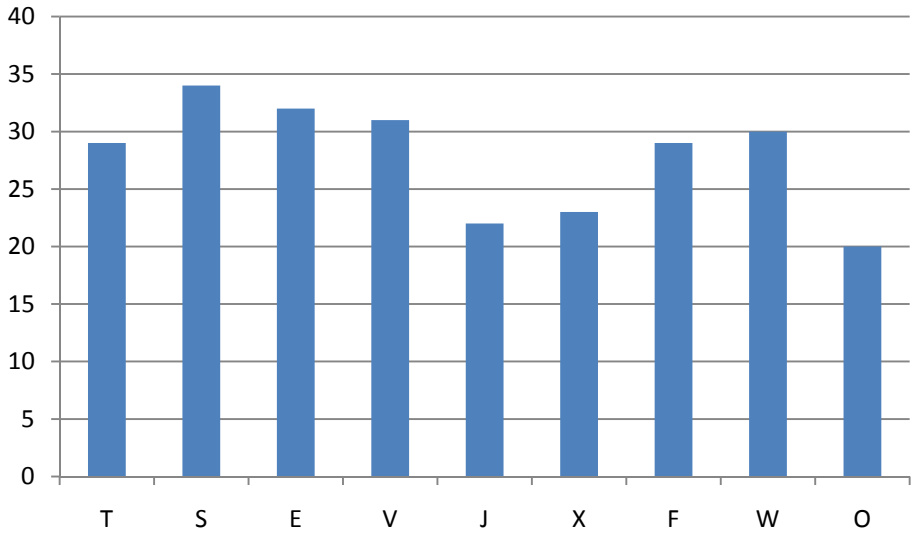

Figure 12: Patterns repetition in the first attempt (choice-based)

2. Choice-based Graphical Password- Second Attempt

At the second attempt, only one participant managed to guess the choice-based graphical password correctly, with other 49 of the participants did not get the required password (Table 9). Figure 13 illustrates the repetition of the objects which were used at the second attempt; it shows that the most objects that were guessed by the participants are; O (fish), then T (flower), S (clock), E (house) and finally X (car).

TABLE 9: Attempt two (Choice-based graphical passwords)

	Frequency	Percent	Valid Percent	Cumulative Percent
correct	1	2.0	2.0	2.0
not correct	49	98.0	98.0	100.0
Total	50	100.0	100.0	

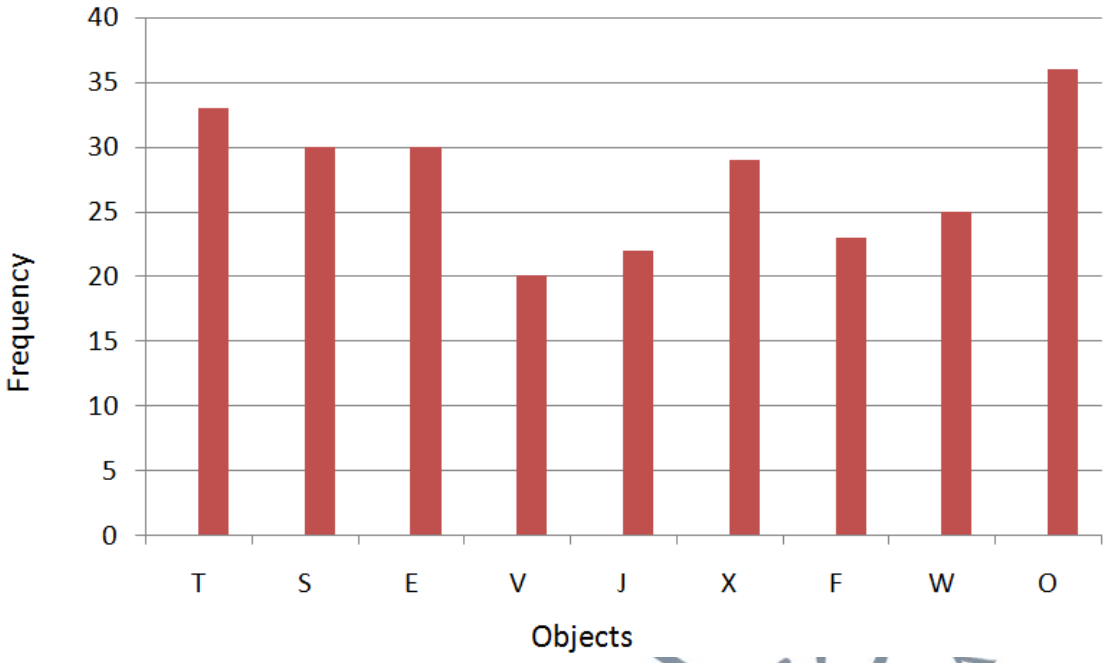

Figure 13: Patterns repetition in the second attempt (choice-based)

3. Choice-based Graphical Password- Third Attempt

At the third attempt, only one participant managed to guess the choice-based graphical password correctly, with other 49 of the participants did not get the required password (Table 10). Figure 14 illustrates the repetition of the objects which were used in the third attempt; it shows that the most objects that were guessed by the participants are; T (flower), E (house), W (faces), O (fish) and X (car) respectively.

TABLE 10: Attempt thee (Choice-based graphical passwords)

	Frequency	Percent	Valid Percent	Cumulative Percent
correct	1	2.0	2.0	2.0
not correct	49	98.0	98.0	100.0
Total	50	100.0	100.0	

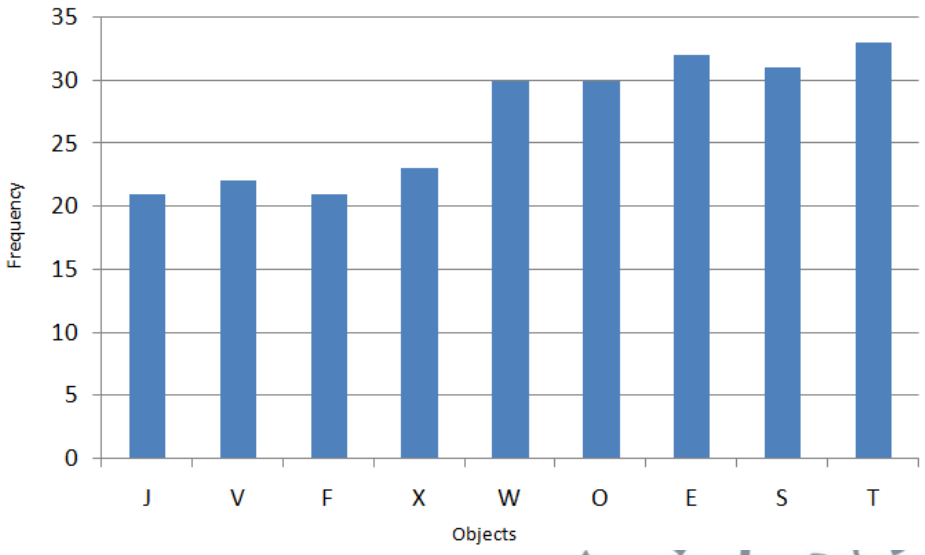

Figure 14: Patterns repetition in the third attempt (choice-based)

4. Compare patterns repetition

Table 11 compares the frequency of the patterns' repetition in the first, second and third attempts to guess the choice-based graphical passwords. In the first attempt, the most pattern that used by the participants to guess the password is s (clock), it was used 34 times. While, T (flower) was the most pattern that used by the participant in the second and third attempts; they were used 33 times in both cases.

TABLE 11: Patterns repetition at the choice-based attempts

	Object's repetition			
Objects	Attempt 1	Attempt 2	Attempt 3	Total
T	29	33	33	95
S	34	30	31	95
E	32	30	32	94
V	31	20	22	73
J	22	22	21	65
X	23	29	23	75
F	29	23	21	73
W	30	25	30	85
O	20	36	30	86

Figure 15 compares the patterns uses in the attempts, where T (flower) was uses the most in the second and third attempts; it was used for 33 times. S (clock) was used the most in the first attempt; it was used 34 times. E (house) was used the most in the first and third attempts; it was used 32 times. O (fish) was used the most in the second attempt; it was used 36 times. W (faces) was used the most in the first and third attempts; it was used 30 times. X (car) was used the most in the second attempt; it was used 29 times. F (cat) was used the most in the first attempt; it was used 29 times. V (coffee) was used the most in the first attempt; it was used 31 times and finally J (butterfly) was used the most in the first and second attempts; it was used 22 times.

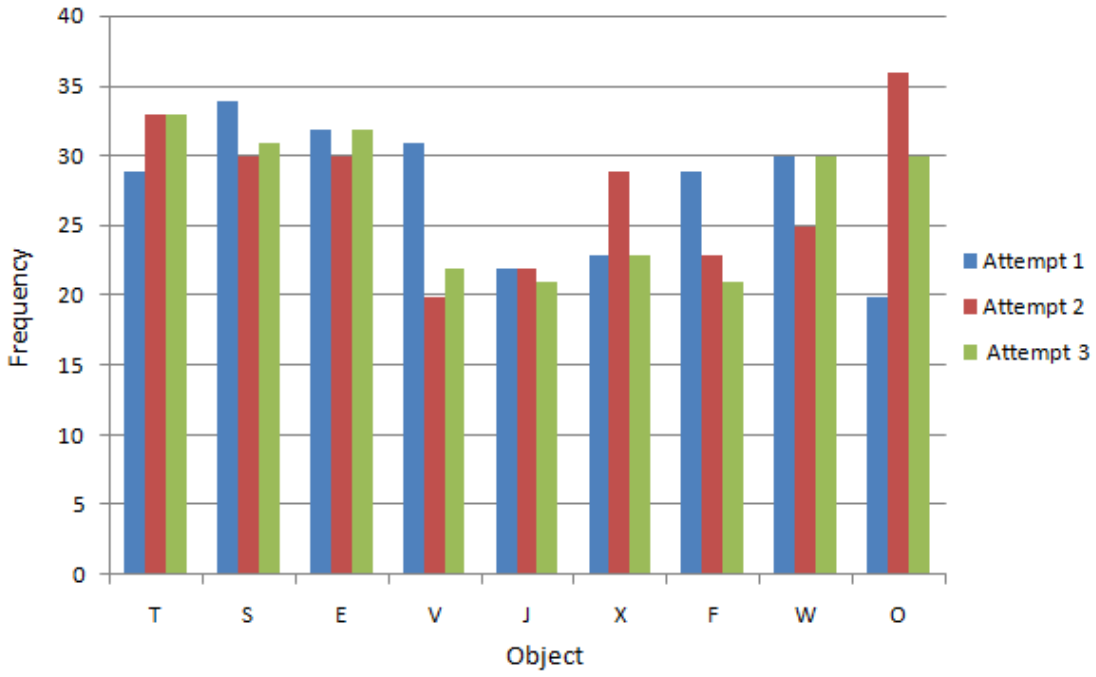

Figure 15: Compare the patterns' repetition of choice-based attempts

Generally, the most objects that were guessed by the participants, at the choice based graphical passwords, as the following sequence; T (flower) it was used 95 times, S (clock) it was used 95 times, E (house) it was used 94 times, O (fish) it was used 86 times, W (faces) it was used 85 times, X (car) it was used 75 times, F (cat) it was used 73 times, V (coffee) it was used 73 times and finally J (butterfly)it was used 65 times.

This was determined by calculating the patterns' frequency for each object in all attempts (Figure 16).

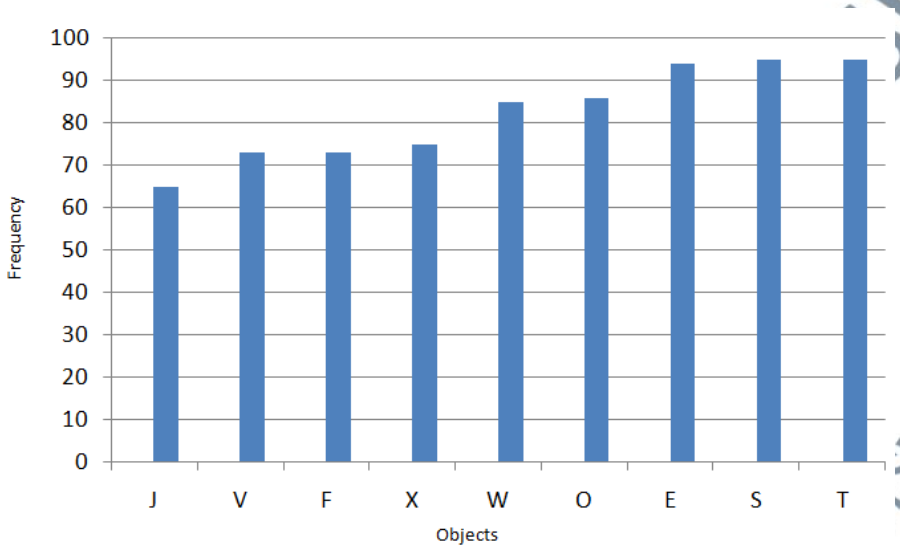

Figure 16: Patterns repetition at the choice-based

4.4.3 Click-Based Graphical Password

The required click-based graphical password consists of five points identified in the second picture in the questionnaire. Each point has its own symbol, so the participants have to write down the symbols for each password. The needed click-based graphical password is (orange bud, white bud, green bud, nose and eye); the participants have to write down the symbol for each object. Therefore, the symbols are; E, F, G, C and D respectively. By comparing the passwords that the participants managed to guess with the correct password that was identified; the results was as the following.

1. Click-based Graphical Password- First Attempt

At the first attempt, only one participant managed to guess the click-based graphical password correctly, with other 49 of the participants did not get the required password (Table 12). Figure 17 illustrates the repetition of the points that were guessed in the first attempt; it shows that the most points that were used by the participants are; D (eye), E (orange bud), C (nose), A (ear) and B (left ear) respectively.

TABLE 12: Attempt one (Click-based graphical passwords)

	Frequency	Percent	Valid Percent	Cumulative Percent
correct	1	2.0	2.0	2.0
not correct	49	98.0	98.0	100.0
Total	50	100.0	100.0	

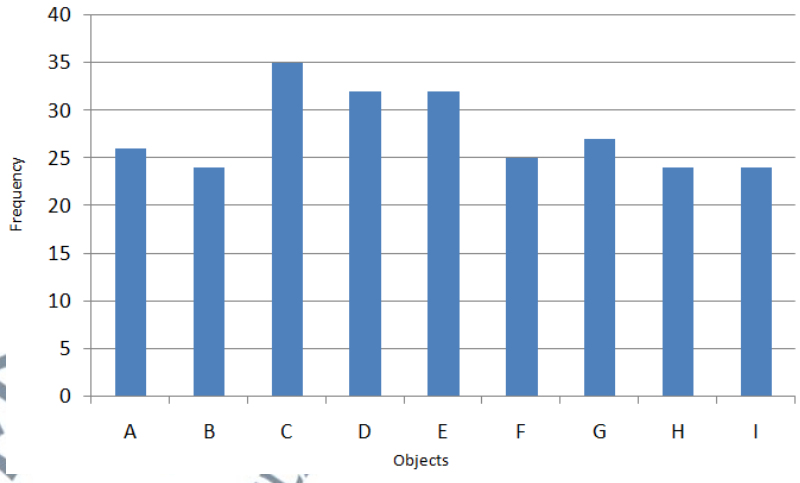

Figure 17: Patterns repetition in the first attempt (click-based)

2. Click-based Graphical Password- Second Attempt

At the second attempt, all the participants did not guess the correct password (Table 13). Figure 18 illustrates the repetition of the points that were used at the second attempt; it shows that the most points that were guessed by the participants are; H (bud), point D (eye), point C (nose), point A (ear) and point B (left ear) respectively.

TABLE 13: Attempt two (Click-based graphical passwords)

	Frequency	Percent	Valid Percent	Cumulative Percent
not correct	50	100.0	100.0	100.0

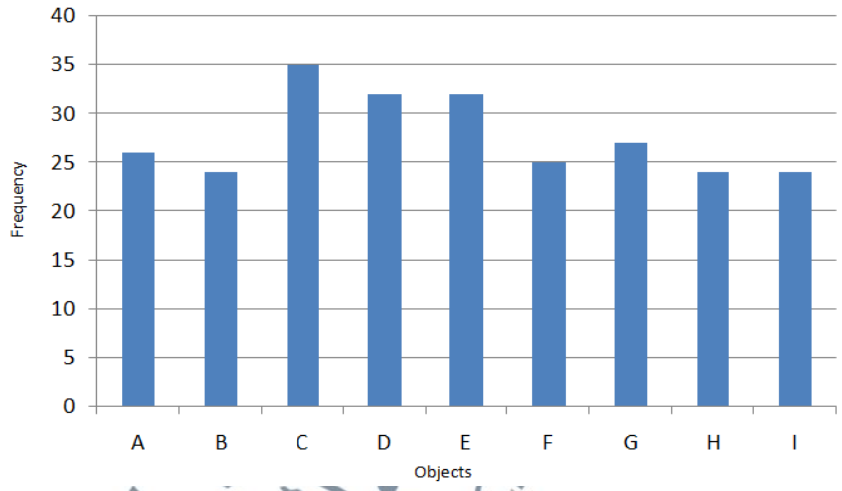

Figure 18: Patterns repetition in the second attempt (click-based)

3. Click-based Graphical Password- Third Attempt

At the third attempt, two participants managed to guess the Click-based password correctly, with other 48 participants did not guessed the correct password (Table 14). Figure 19 illustrates the repetition of the points that were used at the third attempt; it shows that the most points that were guessed by the participants are; C (nose), then D (eye), E (orange bud), H (bud) and finally a (ear).

TABLE 14: Attempt three (Click-based graphical passwords)

	Frequency	Percent	Valid Percent	Cumulative Percent
correct	2	4.0	4.0	4.0
not correct	48	96.0	96.0	100.0
Total	50	100.0	100.0	

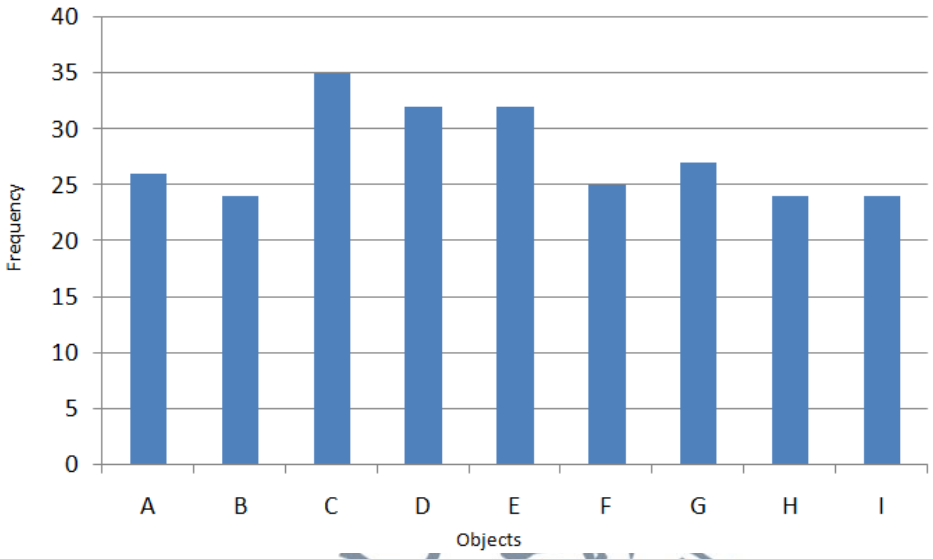

Figure 19: Patterns repetition in the second attempt (click-based)

4. Compare patterns repetition

Table 15 compares the frequency of the patterns 'repetition in the First, second and third attempts to guess the correct click-based graphical passwords. By calculating the frequency of the patterns 'repetition in the First, second and third attempts the most object that were guessed by the participants can be determined. In the first attempt, the most pattern that used by the participant to guess the password is D, it used 38 times. While, H was the most pattern that used by the participant in the second attempt; it used 32 times in both cases. In the third attempt c was used the most, it was used 35 times.

TABLE 15: Pattern's repetition at the click-based attempts

	Object's repetition			
Objects	Attempt 1	Attempt 2	Attempt 3	Total
A	31	30	26	87
B	26	29	24	79
C	34	31	35	100
D	38	31	32	101
E	34	23	32	89
F	25	19	25	69
G	20	27	27	74
H	25	32	24	81
I	17	26	24	67

Figure 20 compares the patterns uses in the three attempts, where D (eye) was used the most in the first attempt, it was used 38 times. C (nose) was used the most in the third attempt, it was used 35 times. E (orange bud) was used the most in the first attempt, it was used 34 times. A (ear) was used the most in the first attempt, it was used 31 times. H (bud) was used the most in the second attempt, it was used 32 times. B (left ear) was used the most in the second attempt, it was used 29 times. G (bud) was used the most in the second and third attempts, it was used 27 times. F (white bud) was used the most in the first and third attempts, it was used 25 times and finally, I (branch) was used the most in the second attempt, it was used 26 times.

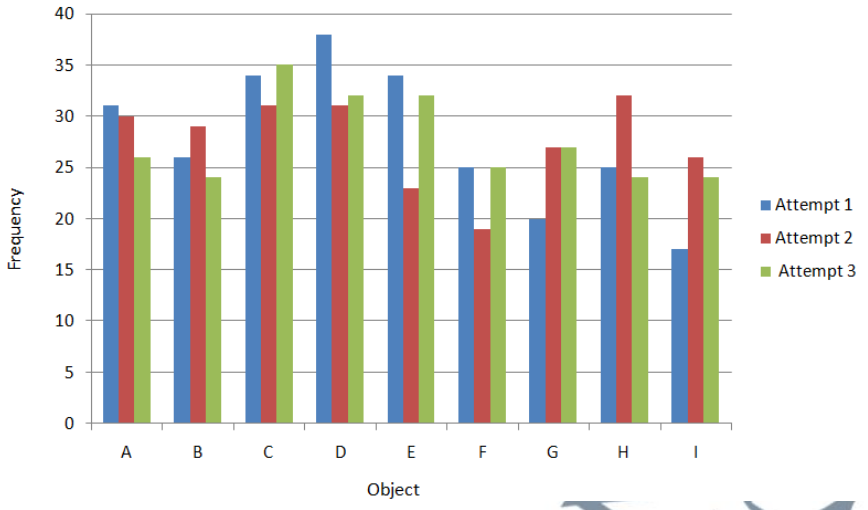

Figure 20: The patterns' repetition at click based (three attempts)

Generally, the most objects were guessed by the participants in the click-based graphical passwords as the following sequence; D (eye) it was used 101 times, C (nose) it was used 100 times, E (orange bud) it was used 89 times, A (ear) it was used 87 times, H (bud) it was used 81 times , B (left ear) it was used 79 times, G (bud) it was used 74 times, F (white bud) it was used 69 times and finally, I (branch) it was used 67 times (Figure 21).

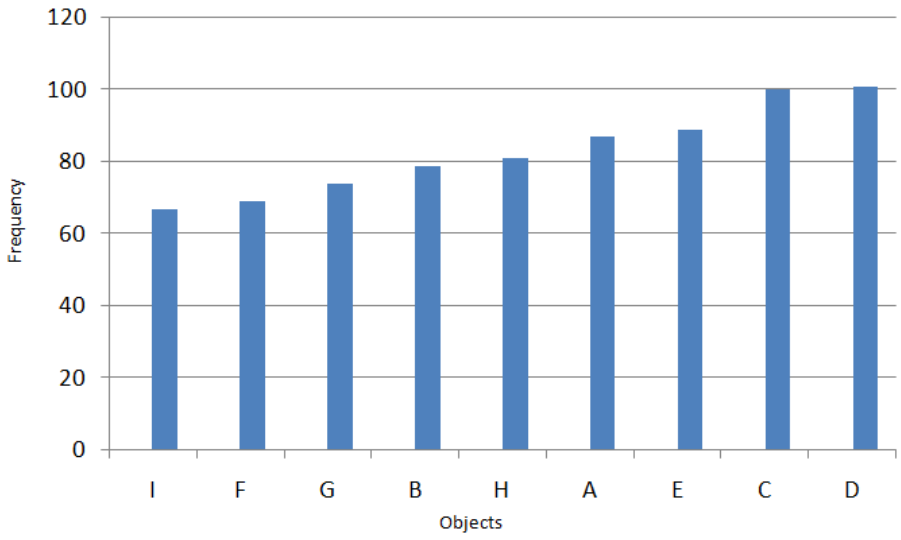

Figure 21: Pattern's repetition at the click-based

4.4.4 The Questionnaire Results

Each password consists of five objects with a sequence order. The needed choice-based graphical password is (fish, butterfly, flower, o'clock and house); the participants have to write down the symbol for each object. Therefore, the sequence order of the objects' symbols is; O, J, T, S and E. The needed click-based graphical password is (orange bud, white bud, green bud, nose and eye); the participants have to write down the symbol for each object. Therefore, the sequence order of the objects' symbols is; E, F, G, C and D. By using SPSS software, version 20 to analyse the data; the results show that only two persons guessed the choice-based graphical password, while three persons guessed the needed clicked based password (Table 16).

TABLE 16: The total correct passwords

	Choice-based Graphical Passwords			**Click-based Graphical Passwords**		
	Attempt 1	Attempt 2	Attempt 3	Attempt 1	Attempt 2	Attempt 3
Incorrect	50	49	49	49	50	48
Correct	0	1	1	1	0	2
Total correct	2			3		

Based on the results, the study can suggest that both passwords types (choice-based graphical password and click-based graphical passwords) have the ability to resist the attacks. However, the choice-based graphical password is better than click-based graphical passwords in resisting the attacks, since the persons who guessed the password at the click-based graphical password is more than the person who guessed the password at the choice-based graphical password.

4.5 SUMMARY

At the first attempt to obtain the needed choice-based graphical password, no one of the participants guessed the password, but in the second and third attempts, only two persons guessed the required choice-based graphical password. Furthermore, in the first attempt to obtain the needed click-based graphical password, no one of the participants guessed the password, but in the second attempt only one person guessed the required password, and two persons guessed the needed password in the third attempt. Based on the results, the choice-based graphical password has more ability to resist the attacks than the choice-based graphical passwords.

The participants use T (flower) and S (o'clock) the most in their attempts to guess the password in the choice-based graphical password. On the other hand, the participants use D (the eye) and C (the nose) the most in their attempts to guess the password in the click-based graphical password.