CHAPTER III

RESEARCH METHODOLOGY

3.1 INTRODUCTION

The main purpose of this chapter is to describe the methodology that is used in the study to collect the data to achieve the research objectives. Generally, comparative evaluation was conducted to determine the best kind of graphical passwords that have the ability to resist the social engineering attacks. The methodology is based on the literature review and survey questionnaire. This chapter also explains the structure of the questionnaire.

Social engineering attacks are understood by referring to the literature review, there are various methods as; attention-grabbing subject, trusted e-mail source, confidence-building, reverse social engineering (RSE), piggybacking tactic, techie talk tactic, a phishing attack, a spear phishing attack, a whaling attack, vishing (voice phishing) attack, social networking sites attacks, neuro-linguistic programming (NLP) attacks and guessing attacks. In this study, the impact of these methods on traditional password and graphical password will be determined, in addition to its impact on the graphical password types.

3.2 PROCEDURE OF THE STUDY

The primary aim of the study is to determine the best graphical passwords type that resists the social engineering attacks. To achieve this aim, a specific procedure was followed at this study. The research procedure is classified into four phases (Figure 5), namely;

1-Phase one: By referring to the literature reviews, the social engineering attack techniques were determined, and later, study its effect on both of the graphical password (GP) and traditional password (TP) from the existing researches (Literature search).

2-Phase two: The social engineering attack techniques, that were collected in phase one, were classified into four groups depending on the exploitation of one of the weaknesses; The first group consists of the techniques that exploiting the victim's confidence, second group consists of techniques based on greed, third group based on the curiosity and the final group based on the human psychology (classification).

3-Phase three: This stage aims to compare and evaluate the effects of social engineering attacks techniques on graphical password types by conducting a study to compare click-based and choice-based methods to obtain an answer of which is more resistant to the social engineering attacks techniques (comparative evaluation).

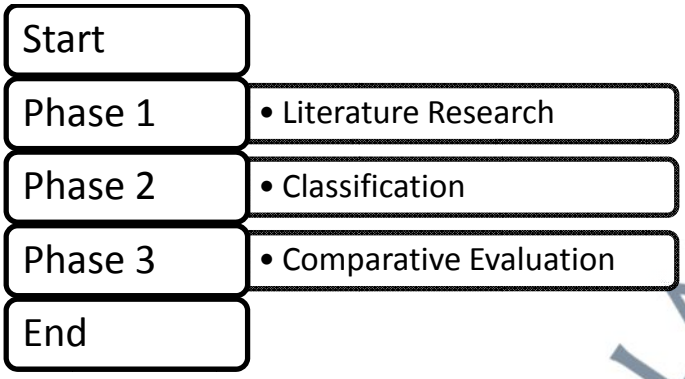

Figure 5: Study procedure

3.3 DATA COLLECTION

This section highlights on the procedure for collecting data. Primary data was obtained by using survey questionnaire, with secondary data was obtained through literature reviews.

3.3.1 Participants

The role of participants was to guess the graphical password (click-based graphical password and choice-based graphical password). Generally, each participant has three attempts to get the choice-based graphical passwords and three attempts to get the click-based graphical passwords.

Simple Random sampling was used to determine the participants; the questionnaire was distributed to 50 participants; as each participant has 6 attempts to get the correct passwords then the overall attempts are 300 which are enough to examine the data via SPSS.

The participants are university students; they were recruited from Universiti Sains Islam Malaysia USIM (Islamic Science University of Malaysia) and Universiti Kebangsaan Malaysa UKM (National University of Malaysia). They were in both undergraduate and postgraduate level. The questionnaires were distributed to the students during their lectures after took the permission from the university.

This study based on the paper to collect the data and personal interviews, it not based on the online questionnaire. Consequently, this needs to determine a close study area to facilitate the collecting data. For this reason Universiti Sains Islam Malaysia USIM and Universiti Kebangsaan Malaysa UKM were chosesn as cases to test the effect of social engineering attack against graphical password.

3.3.2 Structure of the Questionnaire

Based on previous studies such as Jali *et al.* (2011) and Aljahdali & Poe (2013) the questionnaire was developed. Aljahdali & Poe (2013) tested two groups of participants from Saudi Arabia and United Kingdom. Each participant was asked to answer a short questionnaire and then to create a graphical password by choosing 4 pictures from a set of 100 pictures.

Jali et al. (2011) evaluated usability performance when two graphical authentication methods (clicking on image and selecting from a set of images) were combined by using a questionnaire. The questionnaire was distributed to universities students. The questionnaire contained various image so the students can select among them to guess

the password. As a conclusion, they suggested that the method of clicking on images and choosing a series of images can be combined effectively, without significant impediment to users. However, although the results have shown that memorability was maintained, users' clicking accuracy was high, timing was reasonable and users' preference were positive, the trial had also found serious problems.

The steps used to investigate the users' image selection are:

a) Frequency of the most popular themes chosen by users is calculated.

b) For the most popular themes, the most popular image is determined.

c) Identify participants' click areas towards popular images.

d) Determine and investigate the click patterns and hotspot occurrences.

The questionnaire contains four parts (see appendix A): The first part of the questionnaire is an introduction; it explains instructions the participants must follow to answer the questions. The second part is about the participant's demographic; like name, email, study programme (undergraduate or postgraduate), the participants' university and gender. The third part is related to guessing choice-based method. It has nine objects (Figure 6) (choice-based graphical password). Finally, the fourth part related to click-based graphical password method that has a photo with various click points on it (click-based graphical password) (Figure 7).

Figure 6: Choice-based graphical password method

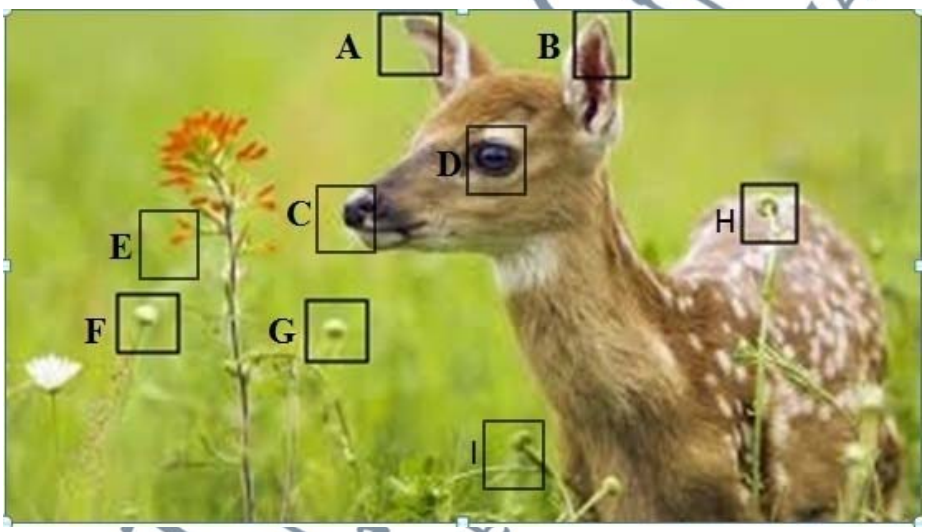

Figure 7: Click-based graphical password method

3.3.3 Steps each participants to do

Each participant had three attempts; at each attempt they must try to guess the needed password. For the choice-based graphical password method, participants had to guess five most popular objects, as there are nine objects.

For the click-based graphical password method there is a determined image, participants had to guess five most popular points in the image. To guess the click-based graphical password each participant had also three attempts. So each participant had six attempts. Since the survey has 50 participants so the overall attempts were 300; 150 attempts to obtain the click-based graphical password and 150 attempts to obtain the choice based graphical password.

The survey was conducted by using a questionnaire to determine the impact of social engineering attacks against graphical passwords types (choice-based graphical passwords and click-based graphical passwords); since the choice-based graphical password and the click-based graphical password depend on choosing from a specific photo unlike draw-based which creates a new drawing by the users.

The needed choice-based graphical passwords and click-based graphical passwords were determined previously, before the questionnaires were distributed. Each password consists of five objects with a sequence order. The first password; is the choice-based graphical password, which 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 second needed password is the click-based graphical password, which are (orange bud, white bud, green bud, nose and eye). Therefore, the sequence order of the objects' symbols is; E, F, G, C and D.

3.3.4 Data Analysis

Data analysis was conducted by using SPSS version 18. The data were collected via the questionnaire analysed by using descriptive statistics to get the correct passwords that the participants guessed. Also, it was used to get the patterns repetition; the most objects that were used by the participants to guess the passwords.

3.4 SUMMARY

This chapter presents a methodology for data collection. Generally, there are three phases, based on the research objectives; namely phases one, phase two and phase three. In phase one, literatures related to social engineering attacks, password authentication and graphical password authentication were collected and reviewed.

In the second phase, classification of social engineering attacks techniques was developed depending on the exploitation of one of the weaknesses; the first group consists of the techniques that exploit the victim's confidence, the second group consists of techniques based on greed, third group based on the curiosity and the final group based on the human psychology.

Finally in the phase three, a comparative study was conducted to obtain the most resistant graphical password type towards social engineering attacks. The next chapter, Chapter IV presents the results and findings from phase three.