CHAPTER II

LITERATURE REVIEW

2.1 INTRODUCTION

This chapter discusses the meaning of social engineering attacks as the way to get unauthorized information and penetrating accounts through the use of non-technical methods rely on the skills of her employer in the ability to deceive others and persuade them to get as much information.

Social engineering involves several methods and techniques 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, guessing attacks and Neuro-linguistic programming (NLP) Attacks. The guessing attack will be utilized as technique in this study, as it is a branch of the social engineering attacks; participants will try to guess the required passwords via a questionnaire.

The Social Engineering Attacks' Cycle has four stages such as; collecting data, relationship building, exploit the relationship and obtain the information. Social

engineering targets the human behaviour to get the required information. Moreover, the chapter explains the traditional passwords and the graphical passwords types and makes a comparison between the effect of social engineering attacks on both of them based on the exists researches.

2.2 SOCIAL ENGINEERING ATTACKS

This section will discuss various ideas that related to the social engineering attacks such as; Social engineering Attacks definitions, Social engineering Attacks techniques and methods, social engineering attacks classification and social engineering attack cycle.

2.2.1 Social Engineering Attacks Definitions

Social engineering has been used to illustrate a number of attacks ranging from widespread phishing for identity information; several researchers try to identify the Social engineering attacks. The term ‘social engineering’ was used in the first by the hacker and it is a common expression for deception people into helping an attacker to contact a target system (Townsend, 2010).

Social engineering is widely used by the attackers since it is the easiest way to obtain access to confidential information or carry out other security-related attacks on information systems (Karpati *et al*., 2012; Mitnick & Simon, 2002).

Harl (1997) defined it as “the art and science of getting people to comply to your wishes”. Whereas, social engineering can be defined as the way to get unauthorized information and penetrating accounts through the use of non-technical methods that rely on the skills of her employer in the ability to deceive others and persuade them to get as much information (Biddle *et al*., 2009).

2.2.2 Social Engineering Attacks Techniques

Social engineering is a process that tries to obtain confidential information. It is a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking people into breaking normal security procedures (Lashkari, 2012; Stobert *et al*., 2010). Social engineering involves several methods and techniques to access the information and penetrate accounts (Shrikala *et al*., 2013; Guenther, 2001).

1- Attention-grabbing subject: One of the most common ways is to try to attract the victim by sending an email to his computer and tell him, for example, the need to upgrade software by clicking on the link, this technique conducted after the attacker obtains the victim confidence (Bakhsi, 2008).

2- Trusted e-mail source: Try to use e-mail by relying on a trusted name and impersonate, this source on the sender whom this method is easy to use and does not require effort and many steps to get the confidence of the victim (Bakhsi, 2008).

3- Confidence-building: It based on obtaining the confidence of the victims. The information is being given to increase the victim confidence, and then ask them by a massage to do something (Danesh *et al*., 2011; Bakhsi, 2008).

4- Trusted domain: By exploitation of the confidence; in this case, the attackers exploit the confidence of the reader of the site and send requests to the reader to follow the link on the page. This link actually is referring to a web page not related to the organization (Chitrey *et al*., 2012; Bakhsi, 2008).

5- Generic Sender: This method is by withholding information about the sender and the development of a generic name. It is best to increase the confidence put the name of the same person to achieve the connection (Bakhsi, 2008).

6- Reverse social engineering (RSE): This method is based on the work of propaganda for the engineer as a social security or technical adviser. This is done through several ways, for example, sending e-mails announce the services provided by or through the business cards at this stage, the social engineer finds a security problem for the company, which will connect to it on the grounds that an expert or security adviser, who in turn tempo damage network connection and access to information and data theft. The attacker at this method gives an impression of fixing a problem (Nelson, 2001).

7- Piggy-backing Tactic: This method also stressed in the engineer impersonating social facilities for example; an important person has the right to access to buildings

and company information. The attackers can exploit the respect of authority and build relationships with victims to gain their trust and get information (Chitrey *et al*., 2012).

8- Techie Talk Tactic: Based on curiosity of the victim; a lot of penetration testing methods and malicious hackers come from a technical background and technique rather than a psychological background. Accordingly, the technicians when it needs to use social engineering; they are choosing the ways in which they know being technical ways; at this method the attacker convince the victim to do something such as give out password (Hunton, 2009).

9- A phishing attack: Phishing attack based on the greed of the victim by sending email messages by the social engineer from project sites known to the general public, such as banking sites or electronic-commerce sites. The person is asked to visit the site or link and the introduction of private and sensitive information such as bank account and password. To convince the person or the victim must appear on the site, it's true, but in fact, the site was created by the attacker (Jagatic *et al*., 2007; Guenther, 2001).

10- A Spear Phishing Attack: This method also depend on the greed of the victim, it based on using information by the social engineer such as the person's name or address; this information will be the first step. And then use this information through the victim included in an e-mail to more legitimate ignorance and reliability of the victim. Also this type based on the curiosity (Guenther, 2001).

11- A Whaling Attack: This type based on the selection of important people in the organization, such as executives or heads of companies. The information about these persons can be obtained easily from the web sites and then used by the attacker to make an attack. Because of the vast amount of information about managers and high-profile targets, whaling is becoming popular because this information makes it so easy for social engineers to target them in a convincing manner.

12-Vishing (voice phishing) attack: This is another type of phishing attacks, but this type does not use the Internet and e-mail, it uses the phone by sending voice messages to the victim's phone or send text messages requesting information from unauthorized or resolve an issue by deceiving these people and it depending on obtain the victim trust and confidence (Danesh *et al*., 2011).

13- Social Networking Site's Attacks: The social networking sites like Face book, Twitter and other sites. These sites are the best environment for the attackers to hunt people and access to information pertaining to them, such as their interests and their workplaces and many others. The researchers show that, most people trust in the friend requests that come by the social networking sites. It's based on the user's curiosity since user try to make a new relationship and knowing a new people (Chitrey *et al*., 2012):

14- Neuro-linguistic programming (NLP) Attacks: NLP is a psychological tool used by social engineers to manipulate people. This method relies on the ability of an attacker to read the physical language and neurological for people targeted and appears to read the reflexes and the ability to observe behavioral patterns of people,

practices, and then exploit all these aspects to gain the trust of the people to get the information.

15- Exploiting the Sex: This way also based on curiosity of the victim to manipulate people to achieve social engineer advantage. In this method the attacker convince the victim by using mutual chemistry which is one of the oldest social engineering tricks in the world (Danesh *et al*., 2011).

16- Exploiting Humans' Problems: This method by exploiting the psychological side of the victims. The attackers follows the victims to gain the information, while the victims are unconscious (screwed). For example; the attackers exploit their presence in bars and exploitation of the mental state of the persons and the situation of loss of consciousness as a result of drinking then the attacker accesses to information (Huber *et al.*, 2013).

17- Guessing attack: It is one of the most important ways of the social engineering techniques. It's based on the ability of the attackers to guess the victim password. This method based on exploiting the confidence of the victim to get the personal information and then to guess the password. So, guessing attack is considered one of the social engineering attacks (Lashkari *et al*., 2012).

2.2.3 Social Engineering Attacks Classifications

Gogolin (2012) classified the social engineering attacks into;

1- Social Engineering Waste Management Attacks;

2- Social Engineering Mobile Device Attacks;

3- Social Engineering Personal Attacks and

4- Social Engineering Reverse Engineers Attacks.

Gogolin identified the main goals of each attack; Waste Management Attacks aim to gather background information about a company (Table 1); familiar Social Engineering Mobile Device Attacks aim to obtain access to the computer systems, capturing wireless transmissions and gets the personal information (Table 2).

Common Social Engineering Personal Attacks (Table 3) aim to gain access to the physical building and computer access. While common Social Engineering Reverse Engineers Attacks (Table 4) aim to obtain the identity theft, information theft and malicious software (Gogolin, 2012).

TABLE 1: Common Social Engineering Management Attacks

Attack goal	Attack vector	Attack discretion	Attack results
Gathering of background information of company	Dumpster diving	The social engineering takes the documents, discarded digital media and other information from external housed waste containers to obtain background information about the company.	Realize of the internal organizational structure and identification of employee, access to customer information and access to confidential or proprietary information.
Gathering of background information of company	Collect documents and information from internal office bins and waste baskets	The social engineering takes the documents, discarded digital media and other information from internal housed office bins or waste basket to obtain background information about the company.	Realize of the internal organizational structure and identification of employee, access to customer information and access to confidential or proprietary information.

Source: (Gogolin, 2012)

TABLE 2: Common Social Engineering Mobile Device Attacks

Attack goal	Attack vector	Attack discretion	Attack results
Obtaining access to the computer system	Shoulder surfing	The social engineer looks over the shoulder of mobile device users at public locations such as airports or Wi-Fi centres and captures their user name and passwords.	Using the captured username and passwords, social engineers are able to attain access to the targeted computer system.
Obtaining	Home worker	The social engineer masquerades as	Using the captured username

access to the computer system		a support technician to capture the home workers username and passwords.	and passwords, social engineers are able to attain access to the targeted computer system.
Obtaining access to the computer system	Mobile applications	The user downloads a mobile games or applications that contain malicious software such as key loggers that allow the social engineer to capture username and passwords.	Using the captured username and passwords, social engineers are able to attain access to the targeted computer system.
Capturing wireless transmissions	Rogue Wi-Fi access point	Social engineer establishes a rogue wireless access point in a public Wi-Fi facility to capture computer transmission including usernames and passwords	Using the captured username and passwords, social engineers are able to attain access to the targeted computer system and obtain personal and corporate information.
Obtain personal information	Vishing	Social engineer sends a mobile voicemail message directing the recipient to contact his or her bank or a company	Capture of personal information and access

Source: (Gogolin, 2012)

TABLE 3: Common Social Engineering Personal Attacks

Attack goal	Attack vector	Attack discretion	Attack results
Gain access to physical building	Tailgating	Social engineer pretends to be a company employee and follows one or more employees into a building bypass access controls	One social engineer has achieved internal physical access, they will be able to obtain documents, digital media and computer access
Gain computer access	Intimidation, persuasion, ingratiation or assistance	The social engineer uses one or more psychological and cognitive techniques to obtain compliance from the target.	Access to computer resources company information and potential loss of funds.
Gain computer access	Alternative techniques	Social engineer uses unexpected or alternative techniques such as windshield flyers to lure targets into accessing a malicious website	Gain access to personal information and resources.

Source: (Gogolin, 2012)

TABLE 4: Common Social Engineering Reverse Engineer Attacks

Attack goal	Attack vector	Attack discretion	Attack results
Identity theft	Telephone	The social engineer receives the user name and passwords of a target being "assisted"	Access to a personal and company information
Information theft	Telephone	Using the user name and passwords provided by the target, the social engineer is able to gain access into the internal computer system	Access to computer resources company information and potential loss of funds.
Malicious software	Telephone	A target is persuaded to access an internet link or download an attachment to help resolve the problem.	The internet site or attachment contains malicious software that infects the company computer system or

			installs software such as a key logger or root kit.

Source: (Gogolin, 2012)

Social engineering attacks can be classified into a number of distinct classes based on the behaviour and possible impact or severity of damages. Also, it can be classified based on; human based and computer based (Hoquea *et al*., 2014).

a- Technology-based approach (computer based) is to deceive the user into believing the he is interacting with a real application or system and get him to provide confidential information. For instance, the user gets a pop up window, informing in that the computer application has a problem, and the user will need to re-authenticate in order to proceed. One the user provides hid ID and password on that pop up window, the damage is done. The hacker who has created the pop up now has access to the user's ID and password and is in a position to access the network and the computer system with credentials of that user.

b- Attacks based on non-technical approach (human based) are perpetrated purely through deception; i.e. by taking advantage of the victim's human behaviour weakness. For instance, the attacker impersonates a person having a big authority; places a call to the help desk, and pretends to be a senior manager, and say that he\ she has forgotten his password and needs to get it rest right away. The help desk person rests the password and gives the new password to the person waiting at the other end of the phone. The attacker now has all the access to perform any malicious activity with the credential of actual user.

By studying the human behaviour (section 2.2.5) in this chapter and based on the literature review, each technique were studied based on the human behavior that were exploited by the attackers; consequently the research classifies social engineering attacks 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.

Exploiting the victim's confidence is an attempt to defraud person or group by gaining their confidence. Whereas, greed means exploit characteristics of the human psyche such as greed. curiosity used to denote the behavior itself being caused by the emotion of curiosity. As this emotion represents a thirst for knowledge, curiosity is a major driving force behind scientific research and other disciplines of human study and human psychology

2.2.4 **The Social Engineering Attack Cycle**

There are several points help social engineers to attack the targets such as; legitimate, importance and sources (Gyorffy, 2009; Almaula, 2008; Allen, 2006).

1- Legitimacy: does the request seem legitimate and usual? For example, should you be asked for this information, and is this how you should normally provide it?

2- Importance: what is the value of the information you are being asked to provide or the task that you are being asked to perform, and how might it be misused?

3- Source: are you confident that the source of the request is genuine? Can you find a way to check?

There is a rough cycle contains the activities that social engineering project follows to gain successful results (Figure 1); this cycle includes four stages are; Foot printing, Establishing trust, Psychological manipulation and the exit (Thornburgh, 2004; Allen, 2006).

1-Collecting data

Collecting data is a method used by the attackers to increase the success of the attacks. It is based on establishing a relationship between the attackers and the individuals who related to the target, so it is considered as a technique of cumulating information that relates to the targets and surrounding environment. This phase collects information about (Thornburgh, 2004; Allen, 2006):

1- A list of employee names and phone numbers
2- Organization Chart
3- Department Information
4- Location information

There are some tools that used to make social engineering engagement easier as; creepy, SET and Maltego. Since the tasks performed prior to doing the social engineering attacks, Foot printing is considered a pre-attack phase.

2- Relationship building

This phase based on obtaining trust from a target after that exploit the victim. It starts by developing a relationship with an employee or anyone working in a business to gain a trust and get information from them, and then the attacker utilizes the information that can harm the business at the next phases (Thornburgh, 2004; Allen, 2006).

3- Exploit the relationship

This phase includes manipulates the trust that has been gained in the previous phase to extract any information related to the target system as sensitive operations performed by the employee himself so it can help the attacker to penetrate into the system (Thornburgh, 2004; Allen, 2006).

4- Phase to obtain information

This phase based on making a clear exit after the information has been extracted without any kind of unnecessary suspicion or proof of his visit so that he/she could be traced-back to his identity (Thornburgh, 2004; Allen, 2006).

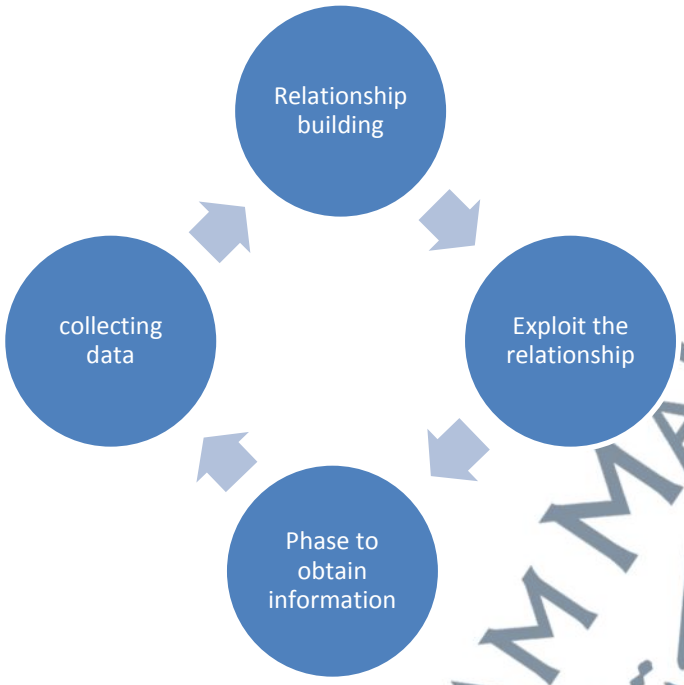

Figure 1: Social Engineering Attack Cycle

Source: Allen, 2006

2.2.5 Human Behaviours

Social engineering targets the human behaviour to get the required information. The human behaviour includes (Gupta & Sharman, 2009); Excitement of Victory, Fear of Authority, Desire to be helpful, Fear of Loss, Laziness, Ego and Insufficient knowledge.

1- Excitement of Victor

This way includes download documents from the target on his own computer this help the document sender to gain remote access to the target machine. For example; Mr. X gets an e-mail stating, "You have won 1 Million Dollars and to claim the winning amount, fill in the attached document and forward it to the email id:

XXXX@XXXX.com. Switch off your antivirus as it may block the download due to highly encrypted Digital Signature of the documents" (Allen, 2006).

2- **Fear of Authority**

On this kind of behaviour, the attackers take the role of authority character, so he/she can easily extract sensitive organizational information from the victims. This action based on that many people trust on authority, and they are anxious in the presence of someone they perceive as an authority figure due to the position and power of the person that intimidates them and makes them (Gyorffy, 2009; Allen, 2006).

3- Desire to be helpful

Keith A. Rhodes, chief technologist at the U.S. General Accounting Office said, "Companies train their people to be helpful, but they rarely train them to be part of the security process. We use the social connection between people, their desire to be helpful".

People in their desire to be helpful and to solve other people's queries, give out a lot of information that otherwise should not be disclosed to an outsider as it could give an attacker a chance to get unauthorized access to the target system causing a possible loss (Allen, 2006).

4- **Fear of Loss**

This case has a lot of examples such as; Mr. (X) gets an e-mail stating, "You have won 1 Million Dollars and to claim the winning amount, deposit $85,000 in Account number: (XXXXXX) in 10 days from receiving this email, failing to which the winning amount would be declared unclaimed and there would be a nee lucky-draw to decide the next winner".

Out of fear that he might lose such a good opportunity, he deposits the amount to the account number provided. When his future replies to the e-mail address go unanswered for the next neither two months nor does the 1 Million Dollar gets deposited to his account, he understands that he has been scammed (Almaula, 2008; Allen, 2006).

5- Laziness

All of us have come across some or the other job that requests us to do only a particular set of actions and not linger around looking for better ways of doing that activity. This causes boredom to the person who performs the same task repeatedly on a daily basis and over the time learns "shortcuts" to do the responsibilities using minimal efforts and still meeting the targets. Such persons over a period of time become lazy and are susceptible to attackers who target such individuals as they know that they would get the required information with much ease due to the laid-back approach of these individuals towards their work (Biddle *et al*., 2009; Allen, 2006).

6- **Ego**

Several times, the attacker makes the person more emotionally sure of himself/herself and thus removing the logical awareness of the security breach that is occurring. The outcome is that, the person being hacked senses no harm in providing whatever it is that the attacker is requesting. The motivation that such an attack succeeds is that the attacker is a receptive audience for victims to display how much knowledge they have (Almaula, 2008).

7- Insufficient knowledge

One of the main issues that differentiate the attacker from other employees of the organization is the knowledge about the target system. It is one of the key factors that differentiate the attacker from other employees of the organization. Several times, because of the lack of appropriate training, the employees are themselves not sure if they have complete knowledge about the product, and Social Engineers take an improvement of such situations by creating a sense of urgency and not allowing the employee much time to think and understanding the fact that they are under attack. The next section will discuss the passwords types that can help to protect the software systems from attacks.

2.3 TRADITIONAL PASSWORDS AND GRAPHICAL PASSWORDS

The password is the most commonly used method for identifying users in computer or communication systems (Soman *et al.*, 2008; Wiedenbeck *et al.*, 2006). Due to the increasing of threats, the alphanumeric passwords are not efficient and safe enough to fully protect the networked computer systems from being compromised by hackers

(Por *et al.*, 2008). If the passwords are difficult to guess by the attackers, then it is safe to use, the users need for secure and memorable passwords. The password problems are either weak or difficult to memorize (Chiasson, 2008).

2.3.1 Text Passwords (Traditional Passwords)

Text password; it is a secret word or characters used for the user's authentication and identity to gain access to resources. But, it is easy to guess and it is vulnerable to attack by dictionary attack and brute attacks, the graphical password can be used as a solution (Soman *et al*., 2008; Wiedenbeck *et al.*, 2006).

In spite of the large number of options for authentication, text passwords remain the most familiar alternative for a number of reasons. The users tend to use the text passwords since it has many advantages such as; Text passwords are easy and inexpensive to implement, and are familiar to most users. Passwords allow users to authenticate themselves without violating their privacy, as biometrics could, since users can select passwords that do not contain personal information (Chiasson, 2008; Renaud, 2005).

The users try to find other kinds of passwords since alphanumeric passwords have some disadvantages as; being hard to remember, vulnerable to "shoulder surfing" problem and easily exposed to dictionary attack since most users tend to choose a common word as their passwords which will be easily guessed (Por *et al.,* 2008).

The reusing passwords across several accounts, using predictable alphanumeric combinations, or storing passwords in an easily accessible, insecure location available the attacker's chance to penetrate the computer systems, but users can solve these problems by using the password managers (Vu *et al.*, 2007; Florencio & Herley, 2007; Sasse *et al.*, 2001; Adams & Sasse, 1999).

2.3.2 Graphical Passwords

The graphical passwords have been proposed as an alternative to text passwords in applications; it's based on graphics and mouse or stylus entry. Graphical password has various types as; choice-based graphical password, click-based graphical password and draw-based graphical password (Wiedenbeck *et al.*, 2005).The idea of graphical passwords based on utilizing images instead of text. The GP methods can be categorized into graphic based GP, spot based GPS and hybrid based GP (Biddle *et al.*, 2009; Por *et al.*, 2008).

A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical password approach is sometimes called graphical user authentication (GUA) (Wiedenbeck *et al.*, 2006). A graphical password is easier than a text-based password for most people to remember.

Users can use the graphical password by several techniques; draw a simple picture in 2d grid, drawing a signature by using the mouse, click on various points on a picture with a specific sequence to create a password or pick several pictures out of many

choices. The security of the system by using the graphical password is very high. On the other hand, the disadvantages for the using of graphical password that the registration and log in process takes a long time and require much more storage space (Soman *et al*., 2008; Wiedenbeck *et al*., 2006).

1- Click-based graphical password scheme

Click-based graphical password scheme consists of various click points on a single image or photo. It has two disadvantages are, the HOTSPOTS and pattern formation attacks. Pass-Points come under click-based graphical password scheme (Shrikala *et al*., 2013).

2- Choice-based graphical password scheme

Cued Click Points and Persuasive Cued Click Points come under click-choice-based graphical password scheme. Cued Click Points were designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Instead of five clicks-points on one image, CCP uses one click-point on five different images (Shrikala *et al.,* 2013; Biddle *et al*., 2009).

By adding a persuasive feature to CCP, PCCP encourages users to choose few predictable passwords, for password creation PCCP uses terms such as the view port and shuffle. To avoid known hotspots the viewport is positioned randomly. The main advantage of PCCP is attackers have to improve their guesses (Shrikala *et al*., 2013).

3- Click-Draw based Graphical Password Scheme

This scheme consists mainly of two steps are; Image selection and Secret drawing. In the first step, an image is selected amongst various images in the image pool. In the second step, the secret is drawn on the selected image. At this scheme the attackers may guess the password. In this technique there is no necessity to remember the sequence of clicks (Shrikala *et al*., 2013; Chitrey, 2012).

2.4 SOCIAL ENGINEERING ATTACKS AGAINST TRADITIONAL PASSWORDS AND GRAPHICAL PASSWORDS

The researchers agree that the traditional passwords are easy to penetrate by all kinds of attack methods such as; Brute force, Dictionary, Guessing, Spyware and loggers, Shoulder surfing and Social engineering attacks (Dunphy, 2013; Lashkari *et al.*, 2012; Khan *et al*., 2011).

Hong *et al.* (2004) study the impact of brute force, dictionary attack, guessing attack, spyware and loggers, shoulder surfing and social engineering attack against graphical password schemes such as; Pass-faces, Blonder, DAS, Pick-o-Lock and Triangle. They summarized the results in a Table 5; the table shows that the graphical password resists the social engineering attacks.

TABLE 5: Possible attack methods on graphical passwords

Graphical password scheme	**Possible Attack Methods**					
	Brute force	dictionary	guessing	Spyware and loggers	Shoulder-surfing	Social engineering
Passfaces	√	√	√	√	√	×
Blonder	√		√	√	√	×
DAS	×	√	×	√	√	×
Pick-o-Lock	√	×	×	√	×	×
Triangle	√	×	×	×	×	×
√= Yes				×= No		

Source: (Hong *et al.*, 2004).

The social engineering attack is less likely to penetrate the graphical passwords since the graphical information is difficult to write down or verbally communicate. The benefits of the graphical password schemes are; including improved recall rates, resistance to information harvesting and resistance to social engineering attacks (Almaula, 2008).

Graphical passwords are less vulnerable to these possible attacks than text based passwords and they believe that it's more difficult to break graphic passwords using these traditional attack methods. Our system is resistant to almost all the possible attacks on graphical passwords (Khan *et al.*, 2011).

Text passwords and alphanumeric information are relatively comfortable to deal with colleagues or attackers. For graphical passwords, a frame of reference must be coordinated to convey the password in sufficient detail for use. This security advantage (complicating social engineering attacks) has usability drawbacks, e.g.,

complicating password reset by phone, and safe backup storage of passwords (Backes *et al*., 2008; Laxton *et al*., 2008; Tari *et al.,* 2006; Roth *et al.,* 2004).

Most texts and graphical password schemes are vulnerable to shoulder-surfing (English, 2012). Shoulder surfing is a targeted attack exacerbated by the visual aspect of graphical passwords. As users enter log-in information, an attacker may gain knowledge about their credentials by direct observation or external recording devices such as video cameras. High-resolution cameras with telephoto lenses and surveillance equipment make shoulder-surfing a real concern if attackers target users and have access to their geographic location (Biddle *et al*., 2011; Backes *et al.,* 2008; Laxton *et al.,* 2008; Tari *et al*., 2006; Roth *et al.,* 2004).

Obtaining graphical passwords is more difficult than text passwords by phishing, since it needs knowledge of users image profiles, the phisher does not know what image to present in order to extract a graphical password (Dunphy, 2013).

Phishing is a kind of social engineering attack; users may be tricked to reveal credentials by any way, e.g., phone calls from a fake help desk or credit company. While, such methods may require targeted background work (or knowledge of personal details in personalized attacks), this is a great deal easier than otherwise breaking into a system (Backes *et al.,* 2008; Laxton *et al.,* 2008; Tari *et al*., 2006; Roth *et al.,* 2004).

Phishing attacks trick users into entering their credentials at a fraudulent website, e.g., the user follows a link, in an email or engineered to return as a search engine result.

As mentioned earlier, phishing attacks on recall- based graphical passwords resemble those on text passwords. Since phishing attacks on recognition-based or cued-recall systems, specific images must be presented to the user. To do so, a phishing site may conduct earlier server probes to collect the images, or may retrieve and relay information from the legitimate site, in a man-in-the-middle (MITM) attack (Dunphy, 2013; Biddle *et al*., 2011; Laxton *et al*., 2008).

Pharming is an advanced form of phishing, subverts the DNS system (by forging DNS responses or DNS cache poisoning) such that domain names are fraudulently resolved to the IP address of an attacker's site (Biddle *et al*., 2011). Social engineering and phishing is more difficult for graphical passwords than for text passwords (Stobert *et al*., 2012). Based on the International Attacks Patterns Standard (CAPEC, 2011) as well as related researches, at present there are common graphical password attacks, namely (Dunphy, 2013; Lashkari *et al*., 2012; Khan *et al*., 2011):

1- Brute Force Attack (BFA): The attack that tries to find every possible combination of the password in order to break it.

2- Dictionary Attack: This method checks for words in a preset dictionary and test whether they are being used as a password or not.

3- Spyware Attack: Spyware installed themselves on a users' computer and records sensitive data for the attacker.

4- Shoulder Surfing Attack: Attackers will peer over a person's shoulder in order to find out their password.

5- Social Engineering Attack (Description Attack) (SEA): An attacker that impersonates an authorized employee by getting information through other employees in the organization.

6- Guessing Attack: This type of attack guesses a user's password by using common personal information such as name of their pets, passport number, family name and so forth.

Text passwords are vulnerable to a range of attacks (Dunphy, 2013; Lashkari *et al.,* 2012; Khan *et al.,* 2011):

1- Replay Attack: the passwords of a legitimate user are reused by an unauthorized person.
2- Social Engineering: an attacker persuades a legitimate user to reveal a password.
3- Observation Attack: an attacker captures a password using simple observation.

Graphical password can be penetrate by shoulder surfing attacks, but graphical passwords are unaffected by traditional key loggers because the keystrokes have been replaced with clicks. Nevertheless, more complex spywares able to capture the screen still can series the user password recognition. Moreover, draw-based graphical password is resistant against dictionary attack, replay attack, password-file compromise attack, the denial-of-service attack, the predictable n attack, and the insider attack (Lin *et al.,* 2007).

Graphical password is claimed to be secure because of these reasons: (1) Enough large password space to be resistant against brute force search attack; (2) Complicated

geometric shapes makes it enough strong to be fraud by shoulder surfing or social engineering; (3) Sufficient warning provided by the layout of the objects to prevent user get into phishing websites. (4) All images can be created fast whenever they are required (Alsulaiman & Abdulmotaleb, 2008)

Click- based graphical password is based on sequential clicks of some points on an image, in which the location and order of the clicks are used as the password. This approach is weak against guessing attacks. Generally, draw-based graphical password is resistant to guessing, traditional key loggers, Weak password, shoulder surfing, while click-based and choice-based graphical password is resistant to dictionary attack, replay attack, password-file compromise attack, the denial of- service attack, the predictable n attack, and the insider attack, it is reparable (Wiedenbeck *et al.*, 2005.

Human brains can process graphical images easily. "A picture is worth a thousand words". Thus, graphical password schemes provide a way of making more human-friendly passwords while increasing the level of security comparing to other types of passwords (Wei-Chi & Maw-Jinn, 2005).

As a conclusion, traditional passwords are easy to attack by all kinds of attacks, while, the graphical passwords are difficult to penetrate in comparative to traditional passwords.

2.5 SUMMARY

Social engineering attacks can be defined as the way to get unauthorized information and penetrating accounts through the use of non-technical methods rely on the skills of her employer in the ability to deceive others and persuade them to get as much information (Biddle *et al*., 2009).

Furthermore, social engineering attacks can be classified into four groups based on the exploitation of one of the weakness's points such as; confidence, greed, curiosity and psychological. Social engineering attacks cycle contains the activities that social engineering project follows to gain successful results, it includes four stages are; Foot printing, Establishing trust, Psychological manipulation and the exit.

There are two main types of passwords are; alphanumeric passwords (Traditional passwords) and graphical passwords. Graphical passwords based on utilizing images instead of text. It has three types: Click-based graphical password scheme, choice-based graphical password scheme and draw-based graphical password scheme. The social engineering attack is less likely to penetrate the graphical passwords since the graphical information is difficult to write down or verbally communicate. In contrast, it is easy to penetrate the traditional graphical passwords by the social engineering attacks.