

# The Impact of Social Engineer Attack Phases on Improved Security Countermeasures: Social Engineer Involvement as Mediating Variable


Louay Karadsheh, Higher Colleges of Technology, Dubai, UAE

Haroun Alryalat, University of Bahrain, The Kingdom of Bahrain

Ja'far Alqatawna, The University of Jordan, Jordan & Higher Colleges of Technology, Dubai, UAE

Samer Fawaz Alhawari, The World Islamic Sciences and Education University, Jordan

Mufleh Amin AL Jarrah, Amman Arab University, Jordan

 <https://orcid.org/0000-0002-3949-6475>

## ABSTRACT

The objective of this paper is to examine a model to identify social engineer attack phases to improve the security countermeasures by social-engineer involvement. A questionnaire was developed and distributed to a sample of 243 respondents who were actively engaged in three Jordanian telecommunication companies. All hypotheses were tested using PLS-SEM. The results of the study indicate that social engineer attack phases (identification the potential target, target recognition, decision approach, and execution) have a partially mediate and significant impact on improving the security countermeasures by social-engineer involvement. On the other hand, the social engineer attack phases (information aggregations, analysis and interpretation, armament, and influencing) have a fully mediate and significant impact on improving the security countermeasures by social-engineer involvement. The findings of this study help to provide deep insight to help security professionals prepare better and implement the right and appropriate countermeasures, whether technical or soft measures.

## KEYWORDS

Attack Approaches, Data Gathering, Information Security, Metadata, Persuasion, Social Engineering

## INTRODUCTION

Today, the internet is the most important communication and information exchange medium. However, securing information and communication systems is still problematic, and no day goes by without a significant cybersecurity incident occurring throughout the world. A recent survey shows that attacks based on tricking victims into performing an action to the benefit of the attacker or sharing sensitive information are one of the most severe threats in cyberspace (Salahdine and Kaabouch, 2019). The human factor has been exploited by SE based upon the context of information security. Therefore, SE is used to launch attacks against data using human factors.

DOI: 10.4018/IJDCF.286762

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

Furthermore, SE can bypass many technical countermeasures through a simple mistake by a user. Cybercriminals use SE tactics because it is usually easier to exploit one's natural inclination to trust than to discover ways to hack the software. The security applications are becoming more complicated and pose a significant challenge for hackers to exploit. For example, it is considerably easier to trick somebody into providing their password than it is for them to attempt hacking systems to steal the password (Jacob, 2014).

The research aims to present a new model of SE attack framework, which describes the attacks more clearly to help security practitioners develop better security countermeasures against SE attacks. The new SE attack framework describes the use of technology and non-technology in clearer steps. The phases included in the proposed SE framework are defined in a logical sequence of measures, including methods and techniques used by SE practitioners and documented in the literature.

Additionally, the society of the 21st century has been defined as presence based chiefly on information and has been initiated upon the conversation of data between completely fields of action. Currently, the quantity of knowledge detained is straight connected to the authority that an individual can have on others (Greavu-Serban and Serban, 2014). Commonly, SE includes an email or other communication that appeals to urgency, fear, or similar emotions in the victim, leading the victim to promptly reveal sensitive knowledge, click a malicious link, or open a malicious file. Since SE involves a human element, preventing these attacks can be delicate for an organization. Additionally, social engineers' IT security enhancement has become a major issue for consultants, managers, and academicians; therefore, the objective of this research is to present a conceptual model in SE attacks.

The rest of the paper is organized as follows: Section 2 discusses the literature review in detail. Section 3 describes in detail the research model and all hypotheses development. Section 4 describes the research methodology in detail. Section 5 presents the data analysis and result. Section 6 present the practical implication of conceptual attack model. Section 7 describes the research originality; Section 8 describes effectiveness of the proposed conceptual model. Finally, conclusion, limitations and future research are addressed in section 9.

## **LITERATURE REVIEW**

### **Concept of Social Engineering (SE)**

There are many definitions of the concept of SE. For instance, Hadnagy (2010) defined SE as the action of operating an individual to take any action that might or can not be in the goal's greatest attention. Additionally, SE is a human creative practice to utilize and transform the objective world; engineering is an artificial system and a product to solve some social-economic problems and improve their living conditions (Zhangbao and Yang, 2019).

An Attacker can automate malicious efforts and reduce attacking costs such as sending phishing or spear phishing emails. Moreover, Mitnick and Simon (2011) claimed that SE usages effect to betray persons by considerable them that the social engineer is somebody he is not. Therefore, the social engineer could have took advantage of people to obtain information with or without the used of technology. To better understand the reason for successful engineering attacks the authors would review the psychological impact.

### **The Psychology of Social Engineering (SE)**

To understand the power of psychology, different terminologies will be explored. The persuasion is an art because it uses high-level communication skills. Persuasion requires asking accurate questions at the right time to influence people to accept your opinion voluntarily without using power (Greavu-Serban and Serban, 2014; Hatfield, 2018). Therefore, to understand why SE successfully exploits the humans, Cialdini's psychology contains the following six codes:

Commitment and consistency occur once the individual creates a decision on something, that the individual wants to be dedicated with the judgement. Additionally, Cialdini (2006) specified that once someone has taken an attitude or accountability it is difficult for them to reverse it.

Authority is when persons usually tend to follow the commands of specialist facts, such as administration and director, several persons obey the authorities, even if they inspire them to action in contradiction to their values or beliefs (Uebelacker and Quiel, 2014; Algarni et al., 2017; Siadati et al., 2017).

Reciprocity is about taking advantage of the human desire to respond kindly to perceived favors. In reality, societies are built on this type of relationship. The power of reciprocity can be so strong that the target would return an even bigger favor than what was received (Uebelacker and Quiel, 2014; Albladi and Weir, 2016).

Social proof is the pressure to follow the crowd. Hadnagy (2010) defined social proof as a psychological occurrence that happens in social circumstances when people are incapable of deciding the suitable type of behavior.

Finally, scarcity is when people are told something they need with limited availability, and to get it, they must fulfill with a confident attitude or action. When something is rare or insufficient, we perceive this as a much higher value (Cialdini, 2006; Kanev, 2017). The key to understanding Cialdini's psychology is that if you can master these principles from a social engineer's perspective, you can influence the victim, which makes it easy to manipulate them.

### **Information Collection Methods (Non-Technical Collection Methods)**

The nontechnical collection methods are used to collect important knowledge through interrelating by the victim without the usage of practical tools or procedures. It relies on psychological handling with the help of fear and trust to get access to sensitive information (Maan and Sharma, 2012; Ahmad, 2017). Furthermore, using their skills, the social engineers use numerous methods such as friendliness, impersonation, conformity, and reverse SE to exploit trust relations and improvement wanted material (Larabee et al., 2006; Flores and Ekstedt, 2016).

### **Information Collection Methods (Technical Collection Methods)**

The attacker uses a variety of technological tools to launch attacks against the victims. For example, vishing is an example of technical collection methods. In vishing, the attackers use the phone system to obtain sensitive information. According to Nagy et al. (2010), vishing can be useful when con artists mimic legitimate ways people interact with organizations. Another type of technical attack is watering holes; the attacker studies the sites most visited by the users. Moreover, baiting attack occurs when a malware-infected storage medium is left in a location where it is likely to be found by victims (Krombholz et al., 2015). Furthermore, another technical means can be clickjacking attacks, which are based on manipulated websites, where HTML elements had been made invisible and put over other HTML elements. Thus, tricking the user into clicking hidden links.

### **Attack Approaches**

There are several attack methods by the social engineer, which will be explored in this section.

The physical approach uses physical means to obtain information such as dumpster diving, theft, extortion (Krombholz et al., 2015), or tailgating.

A physical and technical combined approach occurs when the attacker develops a Trojan horse file and copies it to a USB thumb drive. Then, the attacker can place the infected USB drives in the parking lot of the company. Many curious employees will pick up the USB drives and insert them into their computer systems.

The social approach is considered the most crucial attack approach because it relies on Cialdini's principles of persuasion to manipulate its victims. An example can be authority, reciprocity, liking, and/or scarcity. Furthermore, socio-psychological aspects can be influenced by a person, nature,

demographics variables, and motivations (Algarni et al., 2013), which help to determine the most appropriate target(s), such as the type of user(s).

The technical method is mostly carried out above the Internet (Krombholz et al., 2015). The attacker uses this approach to gather information about the victims online. Furthermore, one famous tool that can be used to facilitate this approach is Maltego (Krombholz et al., 2015). Maltego can be used to gather all security-related work. Other examples are online search, watering holes, or SmiShing.

Socio-technical combines two powerful and effective techniques. Krombholz et al. (2015) provided one example called the baiting attack, which exploits people's curiosity by adding tempting labels. Another common combination of technical and social approaches is phishing (Krombholz et al., 2015; Karakasiliotis et al., 2007) or spear-phishing attacks.

Moreover, the physical-social-technical approach combines the three methods, which is considered as the most potent SE approach and can defeat the latest technical countermeasures. Many banks and other large companies spend large amounts of money on building firewalls and using sophisticated technology to fortify their systems; it is often their employees who are letting social engineers inside (Kapner, 2011). For example, the attacker will attempt to enter the organization's premises by tailgating an employee. Once inside, the social engineer will influence the victim to accept an infected CD or USB drive. This infection might cause the victim's machine to steal the password (Shanmugapriya, 2013), files from the local computer, or becomes part of a botnet. In the next section, different SE attacks strategies and theories will be explored.

## **Attack Strategies**

There are some processes of attack phases that have appeared in several existing process models in SE attack strategies used by social engineers.

In another study by Allen (2006), the attack phase contains of 4 stages. The attack cycles are: Information gathering: a selection of methods can be applied to gather the information related to targets. Developing a relationship: the attacker attempts to establish rapport with the victim to exploit trust. The attacker will position himself as a trusted individual. Exploitation: the attacker manipulates the target to disclose information (e.g., passwords) or perform an action (e.g., creating a new account) that would not commonly occur. This action could be the end of the attack or the beginning of the next stage. Execution: once the victim completed the job necessitated by the attacker, the phase is finished.

Moreover, Cloppert (2009) defined SE attack stages into 6 phases; Reconnaissance: The attacker efforts to gather data from several resources. The methods used are crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies. Weaponization: The process of preparing the malicious payload. For example: linking a remote access Trojan with an exploit into a deliverable payload such as Adobe or Microsoft file as a weaponized deliverable. Delivery: Sending the malicious payload to a target using methods such as email attachments, websites, and USB removable drives. Exploitation: Compromising human vulnerability by targeting an application or operating system vulnerability. Installation: inserting a remote access Trojan or backdoor on the victim system, which allows the attacker to continue presence within the environment. Command-and-Control (C&C): It signifies the period after which opponents leverage the exploit of the system. Exfiltration: Obtaining the data, which involves collecting, encrypting, and extracting information from the victim environment.

Oosterloo (2008) presented a new attack model. This model consists of four phases: The phases are described as: Preparation: the first phase consists of all preparations before engaging a target known as footprinting, including information gathering. Another information gathering technique is based on applying physical attributes. The tactics used are physical reconnaissance, people spotting, dumpster diving forensics analysis, phreaking, phishing, mail-outs, web search, and profiling. Manipulation: a social engineer exploits the trust to manipulate targets in doing what the social engineer wishes to obtain information. The manipulation phase uses influencing to create trust. The manipulation can be performed physically or virtually. Exploitation is the use of the influence on the victim to disclose

information or act in a way, which could result in unofficial access to, unofficial use of, or unofficial revelation of information. The tactics used during this phase can be: physical/virtual impersonation, reverse SE, tailgating, piggybacking, office snooping/desk sniffing, data leakage, and direct approach. Execution. The final phase, when the attacker exploits human weakness. The tactics used are mail-outs, identity theft, and malicious software.

Additionally, the attack model by Laribee et al. (2006) includes strategies of sociability, confidence, determination, impersonation, conformity, dispersion of responsibility, and disruption. With the use of some mixture of these approaches, the social engineer attempts to gain unauthorized access to systems or information with the purpose of committing fraud, network intrusion, industrial espionage, identity theft, or disrupting the system or network.

Finally, a SE attack framework depicted by Mouton et al. (2016) illustrated six-core phases, namely formulation, information gathering, preparation, develops relationships, exploits relationships, and debriefs. The attack formulation phase is used to identify both the goal and target of the specific attack and sources of information. The “goal identification” and “target identification” steps are usually not documented, and very little information on what steps were followed during the “information gathering” phase. The information gathering phase pinpoints all sources of information on both the goal and the target, as well as gather information from the identified sources. In the Preparation phase, all the collected information is combined, and the attack vector is developed. The develop relationship phase is where the attacker begins communication to build a trust relationship with the victim. The exploit relationship phase is used to exploit the target. The final phase is the Debrief phase, in which the victim is gotten out of a primed state during the “maintenance” step, which is used to reassure the victim that he/she is not the prey of a SE attack; and the “transition” step tests, whether the goal has been satisfied. The “transition” step is something only the social engineer knows.

To summarize all the attack strategies above, this research’s purpose is to contribute to this area by looking at the present taxonomy attack strategies. See table 1.

**Table 1. Attack strategies model**

Main Dimension/ Attack strategies	Sub dimension/ Phase of attack strategies							References
	1	2	3	4	5	6	7	
Computer systems	Information Gathering	Developing a relationship	Exploitation	Execution				Cloppert (2009)
Intelligence driven defense	Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command-and-Control (C&C)	Exfiltration	Oosterloo (2008)
Risk of SE	Preparation	Manipulation	Exploitation	Execution				Laribee et al. (2006)
Computer systems	Deception	Influence	Persuasion	Manipulation				Mouton et al (2016)
Communication	Formulation	Information Gathering	Preparation	Develop Relationship	Exploit Relationship	Debrief		Allen (2006)

## PROPOSED MODEL AND HYPOTHESES

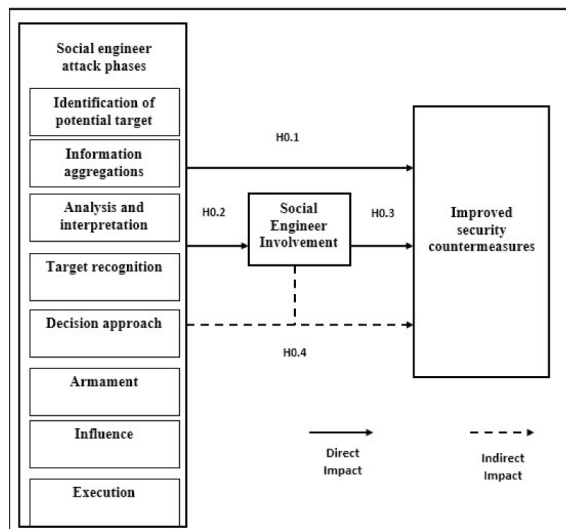
The following research model can be concluded, which consists of three main variable categories that improve security countermeasures. Firstly, independent variables called SE attack phases, which includes eight variables, namely (Identification of potential target, information aggregations, analysis

and interpretation, target recognition, decision approach, armament, influence, and execution). Secondly, mediating variables are called SEI. Finally, dependent variables are called (improved security countermeasures).

Many of the attack concepts discussed lack clarity and detail of the phases performed by the attacker (Allen, 2006; Cloppert, 2009; Oosterloo, 2008; Laribee et al., 2006; Mouton et al., 2016). The summary of research constructs measures is explained in table 2. Furthermore, the researchers found that some researchers placed some technical attacks in the information-gathering phase. However, the technical attacks should follow several phases before it can be used. Moreover, some attack models don't describe what type of tools can be utilized. Furthermore, some attack models jumped from preparation to manipulation without analyzing the information to identify the appropriate target(s). Learning about tools used will help security practitioners implement the most appropriate security controls. Finally, most researchers focus on the victim mindset only and neglect the social engineer's mindset and tactics used. Therefore, the authors will present a new conceptual attack model in Figure 1, that shows the direct and indirect impact of how SEI can integrate with SE attack phases and improve security countermeasures.

Firstly, the authors stated the H0.1 in eight sub-hypotheses as follows:

Figure 1. Hypothesis development



**H0.1.1:** Identification of the potential target has no direct impact on improved security countermeasures.

**H0.1.2:** Information aggregations has no direct impact on improved security countermeasures.

**H0.1.3:** Analysis and interpretation have no direct impact on improved security countermeasures.

**H0.1.4:** Target recognition has no direct impact on improved security countermeasures.

**H0.1.5:** Decision approach has no direct impact on improved security countermeasures.

**H0.1.6:** Armament has no direct impact on improved security countermeasures.

**H0.1.7:** Influence has no direct impact on improved security countermeasures.

**H0.1.8:** Execution has no direct impact on improved security countermeasures.

Secondly, the authors stated the H0.2 in eight sub-hypotheses as follows:

- H0.2.1:** Identification of the potential target has no direct impact on SEI.
- H0.2.2:** Information aggregations has no direct impact on SEI.
- H0.2.3:** Analysis and interpretation have no direct effect on SEI.
- H0.2.4:** Target recognition has no direct impact on SEI.
- H0.2.5:** Decision approach has no direct impact on SEI.
- H0.2.6:** Armament has no direct impact on SEI.
- H0.2.7:** Influence has no direct impact on SEI.
- H0.2.8:** Execution has no direct impact on SEI.

Thirdly, the authors stated the H0.3 as follows:

- H0.3:** SEI has not a direct impact on improved security countermeasures.

Finally, the author stated the H0.4 in eight sub-hypotheses as follows:

- H0.4.1:** SEI has not mediated the impact of identification of potential target on improved security countermeasures.
- H0.4.2:** SEI has not mediated the impact of information aggregations on improved security countermeasures.
- H0.4.3:** SEI has not mediated the impact of analysis and interpretation on improved security countermeasures.
- H0.4.4:** SEI has not mediated the impact of target recognition on improved security countermeasures.
- H0.4.5:** SEI has not mediated the impact of decision approach on improved security countermeasures.
- H0.4.6:** SEI has not mediated the impact of armament on improved security countermeasures.
- H0.4.7:** SEI has not mediated the impact of influence on improved security countermeasures.
- H0.4.8:** SEI has not mediated the impact of execution on improved security countermeasures.

## RESEARCH METHODOLOGY

Using survey data, a quantitative research method was used to investigate how the Jordanian telecommunication company addresses the impact of SE attack phases on improved security countermeasures by SEI as a mediating variable.

### Sample Size

The present study population contains three Jordanian telecommunication companies (N=3); Moreover, the sample size is required to be (384) employees, as mentioned in Sekaran and Bougie (2016); The study sample is shown in table 3.

## DATA ANALYSIS AND RESULTS

### Sample Characteristics

The demographic information is described in table 4.

### Data Analysis

The PLS technique was used in this article using two stages (Anderson and Gerbing 1988). The first phase examined the reliability and validity of variables, while the second phase examined all hypotheses connected to the suggested model.

**Table 2. Research constructs measures**

Construct	Item Code	Measures
<b>Identifying the potential target</b>	Identpota1	Recent hackers identify the target based on return-profit and high rewards
	Identpota2	Hackers attack medical institutions, financial services, retails, industry, utility infrastructure, education institutions, and government organizations.
	Identpota3	Small organization are a possible target by hackers
<b>Information Aggregations</b>	InfoAgg1	Social engineer collects information from non-technical methods such as monitoring company premises
	InfoAgg2	Social engineer collects information from technical methods such as network scanning and mapping using tools
	InfoAgg3	The success of the SE attack in this phase depends upon the amount and quality of information collected.
<b>Analysis and Interpretation</b>	AnandInt1	In this phase, the social engineer analyzes the collected information looking for human vulnerabilities
	AnandInt2	Social engineer uses collected information to learn about the internal working of the company
	AnandInt3	The success of this phase depends upon the type and quality of the information collected in the Information Aggregation phase
<b>Target Recognition</b>	Targetrec1	Average users are an easy target because people vary in their reactions and conducts behavior
	Targetrec2	People are different because of their personality types, hobbies, requirements, and demographic variables, which can be used by taken advantage by attackers
	Targetrec3	Information collected and analyzed can help to develop a very good picture of the target, and what suitable technique needed to identify the right target.
<b>Decision approach</b>	Arname1	The attacker can use social tricks to lure the user into revealing information by establishing a trust relationship to influence the victim.
	Arname2	The attacker can use social-technical, physical-technical or technical (any means) to develop a suitable payload for the chosen victims
	Arname3	The physical-social-technical approach uses different means such as entering the building and convincing victim to insert a USB drive as an example
<b>Armament</b>	Arname1	An attacker needs to prepare a malicious payload using various delivery methods (phishing, sphere-phishing)
	Arname2	The type of attack payload will depend on the kind of the victim(s)
	Arname3	The type of attack payload will depend on the vulnerability of the victim(s)
<b>Influence</b>	Influ1	The attacker can use persuasion (high-level communication skills) by asking accurate questions at the right time to influence victims to reveal information voluntarily
	Influ2	By pretending to be as a top-level role in the company, the attacker can use this privilege to obtain information form victims
	Influ3	The attacker uses reciprocity (the practice of exchanging things with others for mutual benefit) by taking advantage of the human desire to respond kindly to alleged favors
<b>Execution</b>	KMT1	The execution phase is considered as the final phase in the social engineering attack
	KMT2	Execution phase requires the victim to perform an action, for example, clicking on the link rooted in the phishing email as an example
	KMT3	Execution phase essential for violations of data integrity
<b>Social engineer Involvement</b>	SEInvol1	Social Engineer Attack Phases don't need social engineer involvement for successful attack
	SEInvol2	Social Engineer Attack Phases require social engineer involvements from the beginning to the end of phases.
	SEInvol3	The social engineer can help in improving security countermeasures.
<b>Improved security countermeasures</b>	ImpSeCount1	Implementing technical controls without security awareness sessions will not reduce SE attacks
	ImpSeCount2	Implementing security awareness sessions with proper technical controls will reduce SE attacks
	ImpSeCount3	A company needs an annual security awareness training to all users to mitigate SE attacks



**Table 3. Sample size**

Category	Number of Questionnaire Distributed	Number of Questionnaires Returned	Number of Questionnaires Unreturned	Number of Uncompleted Questionnaires Returned	Number of completed Questionnaires Returned
Company 1	130	125	5	8	118
Company2	90	87	3	5	81
Company3	50	47	3	3	44
Total	270	259	11	16	243

**Table 4. Demographic information**

Description	Variable	Result	Percentage
Gender	Male	180	74%
	Female	63	26%
Position	Software development	62	26%
	IT support	103	42%
	Network and infrastructure	43	18%
	Technical operation	30	12%
	Other technical	5	2%
Experience	Less than 2 years	10	4%
	From 2 years to less than 5 years	107	44%
	From 6 years to less than 9 years	92	38%
	From 9 years & more	34	14%
Age	Less than 25	23	9%
	From 25-30 years	84	35%
	From 31-35 years	93	38%
	More than 35 years	43	18%

## The Reliability and Validity of the Model

Firstly, the path loadings (factor analysis results) for the research model are depicted in Figure 2, and the factor can be accepted for analysis if the factor loading for each construct is equal to or greater than 0.50 based on the recommendation by (Hair et al. 2009).

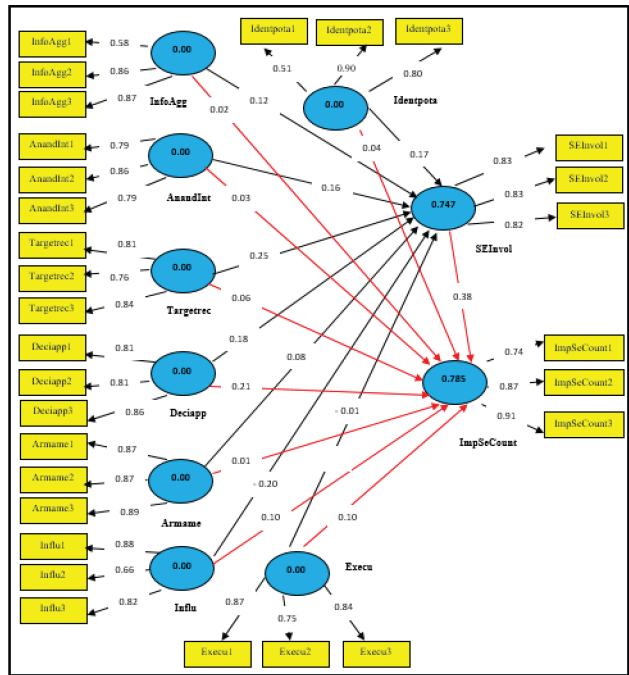
Secondly, CR and AVE analyses were applied to examine all constructs' convergent validity in the suggested model. Fornell and Larcker (1981) recommended that CR's value is bigger than 0.70, whereas the value of AVE is bigger than 0.50 to accept convergent validity. See table 5.

Finally, The mean, std. deviation, skewness, and kurtosis is presented in table 8. The normality issues were not seen for the current data, as proposed by (Sposito et al., 1983; Hair et al., 2009).

Secondly, CA is applied to measure internal consistency (Hair et al., 2009). Note that the construct.

As presented in Table 5, All factor loading for All constructs ranged from 0.90 for Item [Identpota2]: SE attack phases (Identification of potential target) to 0.51 for item [Identpota1] SE attack phases (Identification of the potential target). Therefore, accepted based on the (Hair et al., 2009).

Figure 2. Factor analysis results



Also, as presented in Table 5, the CA values for all constructs ranged from 0.86 for Item namely: SE attack phases (Armament) to 0.61 for Item namely: SE attack phases (Identification of potential target). Thus, all item is internally consistent and accepted based on the orientation of (Saunders et al., 2015).

Furthermore, Table 5 shows the CR values of all constructs ranged from 0.91 for Item, namely SE attack phases (Armament) to 0.79 for Item, namely SE attack phases (Identification of potential target). Thus, all items are exceeding 0.7; accordingly, convergent validity can be accepted for all constructs based on Fornell and Larcker (1981) orientation.

Additionally, the AVE for all constructs ranged from 0.72 for Item improved security countermeasures to 0.63 for Item SE attack phases (Information aggregations). Thus, all constructs in the suggested model are above 0.5; consequently, convergent validity for all constructs can be accepted based on the orientation of (Fornell and Larcker, 1981).

## R-Squared Test

The outcomes of the path quantity method for the suggested model use the R-squared value. See table 6.

Based on table 6, the R-squared assessment for the construct (i.e. Improved security countermeasures) without mediation is 0.764, exceeding 25%, which specified a suitable forecast level in an experimental paper (Gaur & Gaur 2006). Also, the R-squared assessment for the construct (i.e., Improved security countermeasures) through mediation is 0.785, exceeding 25%, suitably based on the orientation by Gaur and Gaur (2006). The R-squared value's measurement growth is 2.1% (from 76.4% to 78.5%) once the SEI is applied as a mediation construct in the relation amongst SE attack phases and Improved security countermeasures. Moreover, the most significant goal construct overall is improved security countermeasures, which displays an R-squared assessment exceeding 0.785 (i.e. the model explains overall improved security countermeasures by 78.5%). The high

**Table 5. The reliability and validity test of the model**

Variables	Item	Factor loading	Cronbach's alpha	CR	AVE	Mean	Std. Deviation	Skewness	Kurtosis
SE attack phases (Identification of potential target)	Identpota1	0.51	0.61	0.79	0.71	4.0590	.64688	-0.440	-0.182
	Identpota2	0.90							
	Identpota3	0.80							
SE attack phases (Information Aggregations)	InfoAgg1	0.58	0.67	0.82	0.63	3.9492	.64117	-0.572	0.394
	InfoAgg2	0.86							
	InfoAgg3	0.87							
SE attack phases (Analysis and Interpretation)	AnandInt1	0.79	0.74	0.85	0.66	3.7270	.74228	-0.932	0.745
	AnandInt2	0.86							
	AnandInt3	0.79							
SE attack phases (Target Recognition)	Targetrec1	0.81	0.77	0.85	0.64	3.9369	.62665	-0.732	0.841
	Targetrec2	0.76							
	Targetrec3	0.84							
SE attack phases (Decision approach)	Deciapp1	0.81	0.81	0.88	0.66	3.7901	.71411	-0.953	1.071
	Deciapp2	0.86							
	Deciapp3	0.86							
SE attack phases (Armament)	Arname1	0.87	0.86	0.91	0.66	4.1207	.73485	-1.074	1.784
	Arname2	0.87							
	Arname3	0.89							
SE attack phases (Influence)	Influ1	0.88	0.70	0.83	0.64	3.9561	.62830	-0.491	.308
	Influ2	0.66							
	Influ3	0.82							
SE attack phases (Execution)	Execu1	0.87	0.76	0.86	0.66	3.9918	.64420	-0.865	1.017
	Execu2	0.75							
	Execu3	0.84							
Social engineer involvement	SEInvol1	0.83	0.77	0.87	0.64	4.0012	.72653		
	SEInvol2	0.83							
	SEInvol3	0.82							
Improved security countermeasures	ImpSeCount1	0.74	0.79	0.88	0.72	3.8380	.75326		
	ImpSeCount2	0.87							
	ImpSeCount3	0.91							

**Table 6. R-squared value**

Factor	R (Square)
SE attack phases on Improved security countermeasures without SEI.	0.764
SE attack phases on Improved security countermeasures with SEI.	0.785

R-squared assessment confirms the suggested model's predictive validity based on the orientation of (Hair et al, 2009).

### Normality Criteria Test

When correlation exists among predictor's, the standard error of predictors coefficients will increase, and consequently, the predictor's coefficients are inflated. The cross-loading is presented in table 7, which shows that all indicators' factor loading is greater than the construct of them on any other factors. Therefore, the validity of the research has been achieved to a satisfactory level.

**Table 7. Square of correlation between latent variables**

	Identification of potential target	Information aggregations	Analysis and interpretation	Target recognition	Decision approach	Armament	Influence	Execution
Identification of potential target	<b>1</b>							
Information aggregations	0.122	<b>1</b>						
Analysis and interpretation	0.039	0.264	<b>1</b>					
Target recognition	0.307	0.239	0.470	<b>1</b>				
Decision approach	0.052	0.242	0.515	0.364	<b>1</b>			
Armament	0.263	0.386	0.220	0.357	0.214	<b>1</b>		
Influence	0.319	0.377	0.454	0.597	0.252	0.311	<b>1</b>	
Execution	0.353	0.255	0.232	0.453	0.440	0.532	0.353	<b>1</b>

The Discriminant validity occurs when one measure in a construct does not correlate with other measures in other constructs. It is recommended that constructs that do not have high correlations provide discriminant validity (Hair et al., 2009). In contrast, correlations between factors were not higher than 0.70. In addition, the values of skewness and kurtosis were not seen to exceed ( $\pm 2$ ). As such, normality issues were not seen for the current data, as proposed by Sposito et al. (1983) .

### Hypotheses Testing

We used a regular examination of the suggested model to offer a complete description of our outcomes and to examine all hypotheses by bootstrapping with smart PLS to find the T-value.

Firstly, it was necessary to find the T-value for the Impact of SE attack phases (Identification the potential target, information aggregations, analysis and interpretation, target recognition, decision approach, armament, influence, and execution) on improved security countermeasures without SEI as a mediating Variable. The T-value for the suggested model is shown in Figure 3. Also, table 8 displays a summary of the outcome.

Secondly, as shown in Figure 4, we found the T-value using smart PLS to examine all hypotheses associated with SE attack phases (Identification of potential target, information aggregations, analysis and interpretation, target recognition, decision approach, armament, influence, and execution) on SEI. Table 8 displays a summary of the outcomes.

Figure 3. Bootstrapping without SEI as a mediating variable

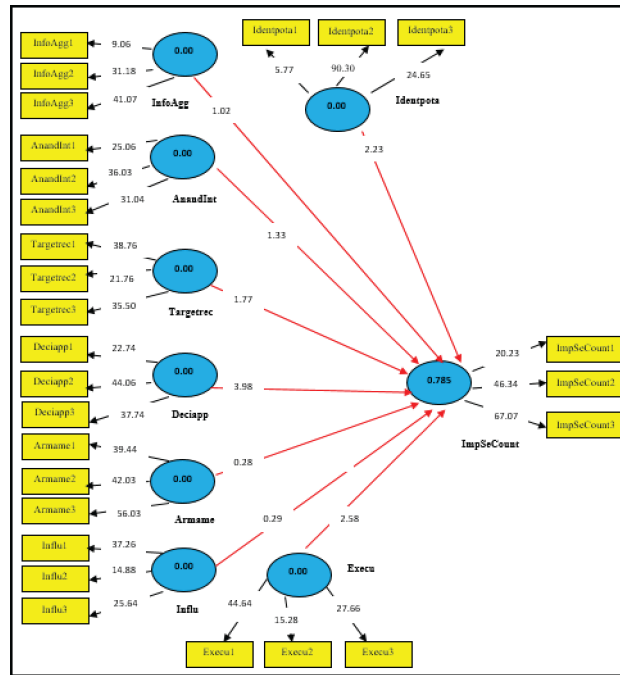
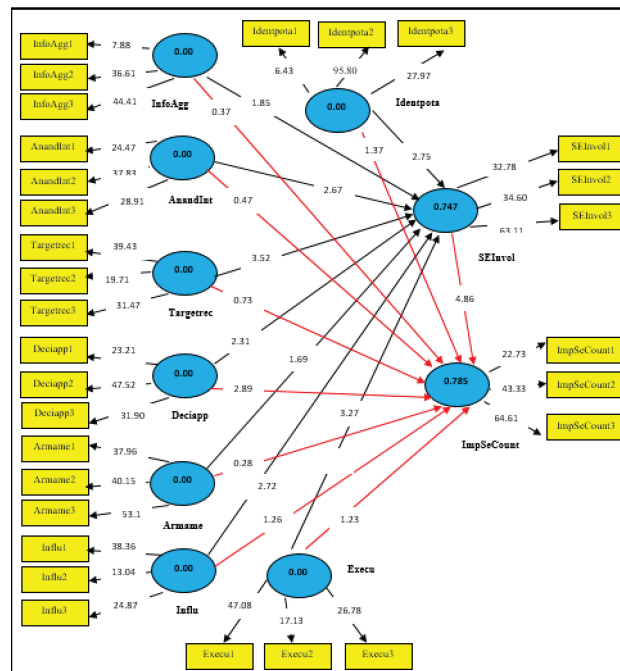


Figure 4. Bootstrapping with SEI as mediating variable



Thirdly, as shown in Figure 4, we found the T-value using smart PLS to examine hypotheses associated with SEI on Improved security countermeasures. Table 8 displays a summary of the outcomes.

**Table 8. Test result first hypothesis**

Relation (direct impact) Hypothetical path	T-value	Beta path coefficient	Interpretation
Identification the potential target → Improved security countermeasures	2.23	0.04	<b>Supported</b>
Information aggregations → Improved security countermeasures	1.02	0.02	<b>Not Supported</b>
Analysis and interpretation→ Improved security countermeasures	1.33	0.03	<b>Not Supported</b>
Target recognition→ Improved security countermeasures	1.77	0.06	<b>Supported</b>
Decision approach → Improved security countermeasures	3.98	0.21	<b>Supported</b>
Armament → Improved security countermeasures	0.28	-0.01	<b>Not Supported</b>
Influence → Improved security countermeasures	0.29	0.10	<b>Not Supported</b>
Execution → Improved security countermeasures	2.58	0.10	<b>Supported</b>
Identification the potential target → SEI	2.75	0.17	<b>Supported</b>
Information aggregations → SEI	1.85	0.12	<b>Supported</b>
Analysis and interpretation→ SEI	2.67	0.16	<b>Supported</b>
Target recognition→ SEI	3.52	0.25	<b>Supported</b>
Decision approach → SEI	2.31	0.18	<b>Supported</b>
Armament → SEI	1.69	0.08	<b>Supported</b>
Influence → SEI	2.72	-0.20	<b>Supported</b>
Execution → SEI	3.27	-0.01	<b>Supported</b>
SEI → Improved security countermeasures	4.86	0.38	<b>Supported</b>

Based on table 8, the T-value amongst (identification of potential target=2.23, target recognition=1.77, decision approach=3.98, and execution=2.58) and improved security countermeasures, exceeding 1.65 (Hair et al. 2009). Therefore, it is significant at  $\alpha \leq 0.05$ . Additionally, based on table 8, the value of beta (identification of potential target=0.04, target recognition=0.06, decision approach=0.21, and execution=0.10) which specifies that the modification of one part in (identification of potential target, target recognition, decision approach, and execution) will yield (0.04, 0.06, 0.21, and 0.1, respectively) a modification in improved security countermeasures. These outcomes do not back hypothesis (H0.1.1, H0.1.4, H0.1.5, and H0.1.8, respectively).

Based on table 8, the T-value amongst (Information aggregations =1.02, analysis and interpretation =1.33, armament =0.28, and influence =0.29) and improved security countermeasures, not exceeding 1.65 (Hair et al. 2009). Therefore, it is not significant at  $\alpha \leq 0.05$ . Additionally, based on table 9, the value of beta (Information aggregations =0.02, analysis and interpretation =0.03, armament =-0.01, and influence =0.10) which specifies that the modification of one part in (Information aggregations, analysis and interpretation, armament, and influence) will yield (0.02, 0.03, -0.01, and

0.10, respectively) a modification in improved security countermeasures. These outcomes do back hypothesis (H0.1.2, H0.1.3, H0.1.6, and H0.1.7, respectively).

Based on table 8, the T-value amongst (Identification the potential target=2.75, Information aggregations=1.85, analysis and interpretation=2.67, target recognition=3.52, decision approach=2.31, armament=1.69, influence=2.72, and execution=3.27) and SEI, exceeding 1.65 (Hair et al. 2009). Therefore, it is significant at  $\alpha \leq 0.05$ . Additionally, based on table 9, the value of beta (Identification the potential target=0.17, information aggregations=0.12, Analysis and interpretation=0.16, target recognition=0.25, decision approach=0.18, armament=0.08, influence=-0.20, and execution=-0.01) which specifies that the modification of one part in (Identification the potential target, information aggregations, analysis and interpretation, Target recognition, decision approach, armament, influence, and execution) will yield (0.17, 0.12, 0.16, 0.25, 0.18, 0.08, -0.20, and -0.01 respectively) a modification in SEI. These outcomes do not back hypothesis (H0.2.1, H0.2.2, H0.2.3, H0.2.4, H0.2.5 H0.2.6, H0.2.7, and H0.2.8 respectively).

Based on table 8, the T-value amongst SEI and improved security countermeasures is 4.86, exceeding 1.65 (Hair et al. 2009). Therefore, it is significant at  $\alpha \leq 0.05$ . Furthermore, the beta value is 0.38, which specifies that the modification of one part in SEI will yield a modification of 0.38 in improved security countermeasures. These outcomes do not back hypothesis H0.3: SEI has no direct impact on improved security countermeasures.

Finally, the statistical analysis results in the last section showed that the smart PLS applied the T value test result to check the variable of SEI is mediating the relationship between SE attack phases (Identification of potential target, information aggregations, analysis and interpretation, target recognition, decision approach, armament, influence, and execution) on improved security countermeasures. See table 9.

Referring to table 9, the T-value between (Identification of potential target, information aggregations, analysis and interpretation, target recognition, decision approach, armament, influence, and execution) and SEI exceeding 1.65 (Hair et al. 2009). Therefore, it is significant at  $\alpha \leq 0.05$ . Moreover, the T-value amongst SEI and improved security countermeasures is 4.86, exceeding 1.65 (Hair et al. 2009). Consequently, it is significant at  $\alpha \leq 0.05$ .

Moreover, T-value between (Identification the potential target, target recognition, decision approach, and execution) and improved security countermeasures exceeding 1.65 (Hair et al. 2009). Therefore, it is significant at  $\alpha \leq 0.05$ . These results have no back hypotheses H0.4.1; H0.4.4; H0.4.5, and H0.4.8. SEI no mediated the impact of (Identification of potential target, target recognition, decision approach, and execution) on improving security countermeasures and therefore, supported partially mediate the relation amongst (Identification the potential target, target recognition, decision approach, and execution) on improving security countermeasures in the Jordanian telecommunication company.

Finally, T-value between (Information aggregations, analysis and interpretation, armament, and influence) and improved security countermeasures not exceeding 1.65 (Hair et al. 2009). Therefore, it is not significant at  $\alpha \leq 0.05$ . These results do not support hypotheses H0.4.2; H0.4.3; H0.4.6, and H0.4.7. SEI no mediated the impact of (Information aggregations, analysis and interpretation, armament, and influence) on improving security countermeasures and therefore, supported Fully mediate the relation amongst (Information aggregations, analysis and interpretation, armament, and influence) on improving security countermeasures in the Jordanian telecommunication company.

## THE PRACTICAL IMPLEMENTATION OF CONCEPTUAL ATTACK MODEL

Tying in with prior research, the authors propose a conceptual attack model to describe how SE attacks succeed. The proposed SE attack model offered more comprehensive and detailed steps than previously published. Therefore, it is essential to become familiar with these SE strategies to combat them effectively and to recognize that strong internal controls are simply not enough (Brody et al.,

**Table 9. Test result from the fourth hypothesis**

Hypotheses	Hypothetical path	Direct effect	Direct effect	Indirect effect	Total effect	Total effect	Interpretation
		T value	Beta Path coefficient	Beta Path coefficient	T value	Beta Path coefficient	
<b>H0.4.1</b>	Identification of potential target → SEI	2.75	0.17		2.75	0.17	<b>Supported</b>
	SEI → Improved security countermeasures.	4.86	0.38		4.86	0.38	<b>Supported</b>
	Identification of potential target → Improved security countermeasures by Social-Engineer Involvement			0.064			<b>Supported Partially mediate</b>
	Identification of potential target → Improved security countermeasures.	2.23	0.04		2.05	0.104	<b>Supported</b>
<b>H0.4.2</b>	Information Aggregations → SEI	1.85	0.12		1.85	0.12	<b>Supported</b>
	SEI → Improved security countermeasures.	4.86	0.38		4.86	0.38	<b>Supported</b>
	Information Aggregations → Improved security countermeasures by Social-Engineer Involvement			0.045			<b>Supported Fully mediate</b>
	Information Aggregations → Improved security countermeasures.	1.02	0.02		0.99	0.065	<b>Not Supported</b>
<b>H0.4.3</b>	Analysis and Interpretation → SEI	2.67	0.16		2.67	0.16	<b>Supported</b>
	SEI → Improved security countermeasures.	4.86	0.38		4.86	0.38	<b>Supported</b>
	Analysis and Interpretation → Improved security countermeasures by Social-Engineer Involvement			0.060			<b>Supported Fully mediate</b>
	Analysis and Interpretation → Improved security countermeasures.	1.33	0.03		1.27	0.09	<b>Not Supported</b>
<b>H0.4.4</b>	Target Recognition → SEI	3.52	0.25		2.67	0.16	<b>Supported</b>
	SEI → Improved security countermeasures.	4.86	0.38		4.86	0.38	<b>Supported</b>
	Target Recognition → Improved security countermeasures by Social-Engineer Involvement			0.095			<b>Supported Partially mediate</b>
	Target Recognition → Improved security countermeasures.	1.77	0.06		1.95	0.155	<b>Supported</b>

*continued on next page*

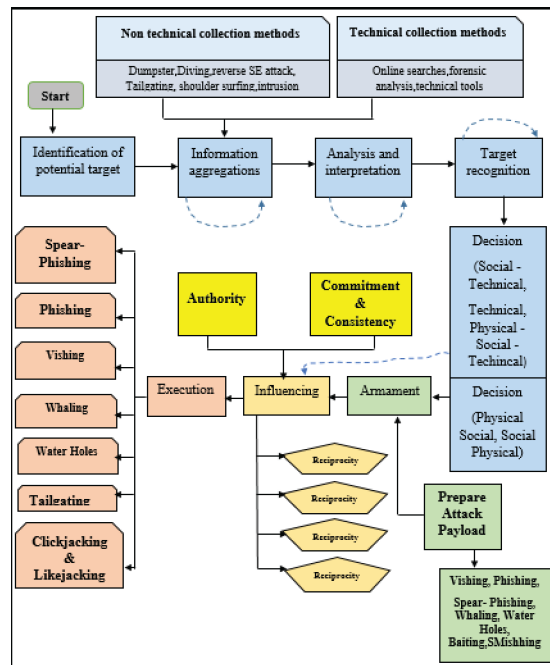


Table 9. Continued

Hypotheses	Hypothetical path	Direct effect	Direct effect	Indirect effect	Total effect	Total effect	Interpretation
		T value	Beta Path coefficient	Beta Path coefficient	T value	Beta Path coefficient	
<b>H0.4.5</b>	Decision approach → SEI	2.31	0.18		2.31	0.18	<b>Supported</b>
	SEI → Improved security countermeasures.	4.86	0.38		4.86	0.38	<b>Supported</b>
	Decision approach → Improved security countermeasures by Social-Engineer Involvement			0.068			<b>Supported Partially mediate</b>
	Decision approach → Improved security countermeasures.	3.98	0.21		3.83	0.278	<b>Supported</b>
<b>H0.4.6</b>	Armament → SEI	1.69	0.08		1.69	0.08	<b>Supported</b>
	SEI → Improved security countermeasures.	4.86	0.38		4.86	0.38	<b>Supported</b>
	Armament → Improved security countermeasures by Social-Engineer Involvement			0.030			<b>Supported Fully mediate</b>
	Armament → Improved security countermeasures.	0.28	-0.01		0.28	0.02	<b>Not Supported</b>
<b>H0.4.7</b>	Influence → SEI	2.72	-0.20		2.72	-0.20	<b>Supported</b>
	SEI → Improved security countermeasures.	4.86	0.38		4.86	0.38	<b>Supported</b>
	Influence → Improved security countermeasures by Social-Engineer Involvement			-0.076			<b>Supported Fully mediate</b>
	Influence → Improved security countermeasures.	0.29	0.10		0.34	0.024	<b>Not Supported</b>
<b>H0.4.8</b>	Execution → SEI	3.27	-0.01		3.27	-0.01	<b>Supported</b>
	SEI → Improved security countermeasures.	4.86	0.38		4.86	0.38	<b>Supported</b>
	Execution → Improved security countermeasures by Social-Engineer Involvement			-0.003			<b>Supported Partially mediate</b>
	Execution → Improved security countermeasures.	2.58	0.10		2.24	0.097	<b>Supported</b>

2012). The authors have proposed and developed a conceptual SE attack framework model, as shown in Figure 5. The proposed framework was developed based on several literature research works by examining different attack models, white papers, technical papers, and known attack techniques. The objective is to scrutinize previous researchers' contribution critically and explain different views of earlier research initiated within research flows. Based on the literature reviews and conceptual model presented previously, the proposed SE attack model includes the eight main phases described as follows: By summarizing prior research, we can understand how different attack methods are executed according to the authors, which helped develop an enhanced attack model displayed in Figure-5.

Figure 5. Practical implementation of conceptual attack model



Based on the literature reviews and conceptual model presented previously, the proposed SE attack model includes the eight main phases described as follows:

The first phase is about identifying the potential target. Currently, social engineers are concentrating their efforts on targets with high rewards, such as medical institutions, financial services, retails, industry, utility infrastructure, education institutions, and government organizations. The motivation can be monetary gain, self-interest, revenge, and/or external pressure (Allen, 2006). The target can be a large organization because the impact or return profit will be high. Another possible target is a small organization because it is easier to infiltrate them due to less complicated security implementation, and they can be used to penetrate a larger supplier.

The second phase is information aggregation: through this stage, the social engineer will gather data from several resources such as nontechnical and/or technical methods. This phase's importance is that the more information the social engineer aggregates, the more attack vectors options can be developed, the attacker understands better the target's weaknesses and strengths (Hadnagy, 2010). This phase may also include network scanning, network mapping, monitoring company premises, or search the Company's trash (Medlin et al., 2008; Sarriegi and Gonzalez, 2008). For example, the

Maltego application permits the social engineer to aggregate information, data, people, websites, or companies and categorizes the composed information into a user-friendly format using a graphical user interface, which is easy to read and utilize.

The third phase is the analysis and interpretations phase: the social engineer will analyze the collected information observing for human weaknesses (Algarnietal.,2013) to be subjugated. Therefore, social engineers can use any captured information to obtain valuable knowledge of the corporation's internal workings and then usage this information to design the attack consequently (Brody et al., 2012).

The fourth phase is target recognition: the social engineer attempts to identify the most suitable victim(s) based on the first phase's selected company. The type(s) of a user(s) will depend on the target company and information value. Average users are easily targeted because people vary in their reactions and conducts, and their vulnerabilities also differ from each other (Algarni et al., 2013). These differences are because of distinctive personality types, hobbies, requirements, and demographic variables such as age, gender, and educational levels (Algarni et al., 2013). All this information can help to develop a broad picture of which type of target needs to be focused on and the suitable technique required to identify the right target. Once the attacker acknowledged the right target(s), the attacker will move to the next phase of the attack.

The fifth phase is the decision: the approach can be either physical, technical, physical-technical, social, social-technical, or physical-social-technical. The social engineer will decide the most appropriate approach depending on the result from the information collected and analyzed and the victim identified. Depending on the chosen method, the following step will be either the Armament phase or the Influence phase. If the attack doesn't require creating or developing technical tools, then the subsequent step will be the Influence phase. The Influence phase will be fed by either social, physical, or physical-social approaches. This phase is divided into three options:

**Option 1:** Can be either physical or social or a combination of both. If the social engineer found a weakness in physical security within the building, then the attacker may choose to tailgate, for example. Another option is to employ Cialdini's principles of persuasion to influence victims to obtain information by establishing trust. Once trust is established, the attacker can exploit this faith to trick the victim into saying "yes" to the hoax (Algarni et al., 2013).

**Option 2:** It can be either social-technical, physical-technical, or technical. For example, once the attacker has a full picture of the vulnerability of the victims. The attacker might decide to adopt the phishing attack. This requires the attacker to develop a suitable payload for the chosen victims in the next phase. This example is more of a social-technical approach. On the other hand, a purely technical approach can utilize baiting attacks or crafting phishing emails. Finally, this option's output will go to feed the Armament phase to prepare the attack payload.

**Option 3:** It can be a physical-social-technical approach. In this process, the attacker will attempt to tailgate; by pretending to be a technician and persuade the victim to insert a USB drive with an infected keylogger. The social engineer makes the victim believe that the keylogger is some trusted application and makes him insert it (Shanmugapriya, 2013). The result of this option will lead to the Armament phase to prepare the attack payload and proceed forward in attack phases.

The sixth phase is concerned with the armament: the social engineer will prepare the target's appropriate attack payload. The possible attack payload type might be phishing, sphere-phishing, vishing, SmiShing, and/or baiting. In this phase, the attacker will develop a remote access Trojan containing an exploit into a deliverable payload. Progressively, client application data files such as Adobe pdf or Microsoft Office documents assist as a weaponized deliverable (Hutchins et al., 2011). The three most widespread distribution vectors for weaponized payloads by APT performers, as perceived by the Lockheed Martin Computer Incident Response Team (LM-CIRT) for the years 2004-2010, are email attachments, websites, USB removable media (Hutchins et al., 2011) or email with URL link. The malicious attachment or URL link will be created as a form of phishing email

or spear-phishing email. The SE toolkit can customize different attack vectors by cloning a website such as Facebook, Gmail, Twitter, or Yahoo in order to trick the victim into clicking on the embedded link to steal user credentials. If the attacker learns that the user can access Facebook's accounts from inside the company. Then the link may contain a fake link to Facebook's web page. Once the malicious payload is ready, the attacker will proceed into the influence phase to convince the victim to click on the link.

The seventh phase is influence: the social engineer will choose one or more of Cialdini's persuasion codes' principles. Choosing any one of these codes will depend on the previous phases. Furthermore, the social engineer will establish a trust relationship with the victim(s). Moreover, SE attacks often work because trust is exploited (Gulenko, 2013), making trust relationships is the key to success. The social engineer will cultivate a good strategy to achieve that goal, such as "pretexting," in which a social engineer crafts a strategy designed to encourage the victim to fall for the trick (Workman, 2008). Once the trust is established, the victim will become vulnerable, and the attacker will move to the next phase. The success of transmission of the armament to the targeted environment (Hutchins et al., 2011) will rely on the collected information and the attacker's skill to lure the victim. An example of influencing might be time pressure or scarcity, which can impact people's choices. It influences the logical operations of human decisions; therefore, the victim is easily trapped to accepting arguments that should be challenged (Petty et al., 2002).

The final phase is called the execution: assuming the attacker created a phishing email and convinced the victim to click on the link embedded in the phishing email, the exploitation triggers intruders' code (Hutchins et al., 2011). This causes the victim's machine to be infected with a malicious file and connect the machine to the attacker system. The compromised system will beacon outside to a command and control system located somewhere to establish a covert communication channel (Hutchins et al., 2011). Once the victim machine is connected, the social engineer will attempt to steal information or execute privilege escalation. Once this phase is concluded successfully, the attacker succeeds in stealing data, breaching confidential, or worse. In this case, the attacker succeeded in achieving the goal.

## **RESEARCH ORIGINALITY**

To better understand the proposed attack model compared to previous literature reviews, the authors will examine five attack models from the literature, see Table 13.

The first attack method (Allen, 2006) focuses on developing then the relationship to get someone to act by manipulation; however, this model doesn't explain why this target was chosen, not clear how the information was analyzed, and on what basis the exploitation was carried out.

The second attack method (Cloppert, 2009) emphasizes the actual cyber-attacks and exploiting victims using technology means; however, this model doesn't elaborate on why the target was chosen, analysis of data collected is missing, and how the decision was made.

The third attack method (Oosterloo, 2008) is based on the recurring and iterative process for describing the four basic phases of SE attacks; however, it is not clear in the attack model why the main target was selected; how the aggregated information was analyzed, how the decision is made, and selection of the right attack payload. Therefore, the jump from the Preparation phase to the Manipulation phase requires identifying the right target and making the right decision on which approach must be used to guarantee a successful attack.

The fourth attack method (Laribee et al., 2006) focuses on using influencing victims to encourage them to act differently and according to the social engineer's desire. Furthermore, the author created two separate models: the attack and trust, instead of combining them together. Since the success of the offense depends upon the level of confidence. Therefore, combining both during the phases will help to describe the attack process clearly, and why the attack succeeded. Furthermore, the toolkits listed are not mapped to the proposed phases. The tools need to be mapped to describe to the reader which

applicable one for each phase and how to defend against them. Moreover, the main attack categories listed can be combined and categorized under influence the phase because deception, persuasion, and manipulation goals to change the victim to act upon social engineer goals.

The final attack model by Mouton et al., 2016 described the planning and flow of the full attack briefly, but without a description of technical or nontechnical techniques applied. Furthermore, it doesn't explain what type of attack approach is appropriate to the target, why and how the target was selected, and what type of armament is necessary and how it will be delivered.

**Table 10. Summary of current attack models with the proposed model**

<b>Proposed Attack Model</b>	<b>Allen (2006)</b>	<b>Cloppert (2009)</b>	<b>Oosterloo (2008)</b>	<b>Laribee et al. (2006)</b>	<b>Mouton et al. (2016)</b>
Identification	X	X	X	X	Attack formulation
Information aggregations	Information gathering	Reconnaissance	Preparation	X	Information gathering
Analysis and interpretation	X	X	X	X	Preparation
Target recognition	X	X	X	X	X
Decision	X	X	X	X	X
Armament	X	Weaponization; Delivery	X	X	X
Influence	Developing relationship	X	Manipulation	Deception; Influence; persuasion; manipulation	Develop relationship
Execution	Exploitation; Execution	Exploitation; Exfiltration	Exploitation; Execution	X	Exploit relationship; Debrief

This proposed model is unique compared to other models described in the literature reviews. It discusses the use of technology and non-technology in clear steps than other attack models. Furthermore, this model breaks down the phases in more detail to provide a better understanding of SE attack methods. Every phase is described in detail with possible tools and methods identified and used. Additionally, the proposed model takes the reader into a logical sequence of steps used by SE attackers. This logical sequence of steps helps the reader to understand the motivation and techniques used exclusively in every step. Finally, the proposed attack model contains two phases not declared by previous literature: Target recognition and decision. Additionally, the introduced attack model identifies missing phases in previous literature, which is explaining the attacker steps. By exploring the earlier research studies and based on the researchers' best knowledge, no effective research in the area of the SE attack process was found in the logical and detailed sequence of steps, which mimic the actual activities performed by the SE attackers. Therefore, this paper fills this gap in the literature by examining the phases in more detail.

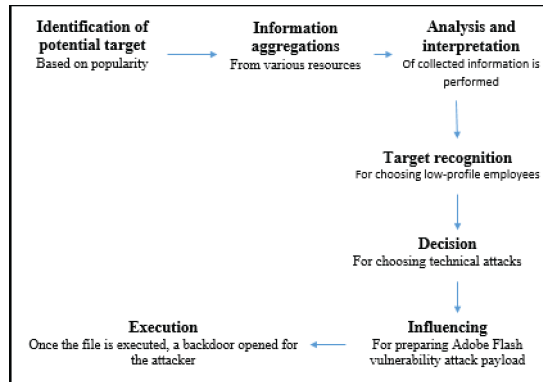
## EFFECTIVENESS OF THE PROPOSED CONCEPTUAL MODEL

The other attack framework models didn't describe the actual attack phases in clear steps. Some of the literature reviews missed some phases or focused on specific phases and ignored others. Therefore, the authors chose Rivest–Shamir–Adleman (RSA) SecurID breach to attempt to map the attack to the proposed attack framework. This breach hit the media all over the world due to its high impact on many worldwide companies. The RSA breach is a combination of high-tech and low-tech.

- **Identification:** The attackers picked RSA because the organization is widespread and gives SecurID items, which 40 million organizations worldwide utilize. RSA is a prominent IT security merchant in charge of assembling and conveyance of its SecurID tokens.
- **Information aggregation:** According to Jon Oltsik, a principal analyst with the Enterprise Strategy Group, "I think that the intelligence gathering and setup lasted awhile," he told eWEEK. Because of being a popular company, it was easy for the attacker to gather the information from various resources, e.g., employee, newspapers, digital media, and social networking sites etc.
- **Analysis and interpretation:** Based on the information collected, the attackers analyzed the collected information looking for human vulnerabilities and appropriate target(s). This stage required careful analysis of the collected information to look for a breach into the system.
- **Target recognition:** Two small groups of employees were chosen. None of the targets picked were individuals who might ordinarily be viewed as high-profile targets, for example, an official or an IT manager with special network privileges.
- **Decision:** The attackers chosen phishing email as a method to launch the attack. The attackers chose to send two diverse phishing emails over two days to the targets, which as per the model, falls in the technical category.
- **Armament:** A phishing email with a zero-day exploit was created. The email subject line read '2011 Recruitment Plan.' "The email contains an excel file titled '2011 Recruitment plan.xls.' "The spreadsheet contained a zero-day exploit that installs a backdoor through an Adobe Flash vulnerability (CVE-2011-0609).
- **Influencing:** The email was crafted well enough to deceive one of the employees to retrieve it from their Junk mail folder and open the attached excel file. The attackers spoofed the e-mail to appear to come from a "webmaster" at Beyond.com, a job-seeking and recruiting site. Inside the e-mail, there was just one line of text: "I forward this file to you for review. Please open and view it."
- **Execution:** Once the target clicked on the file, the attacker got inside the network, control the machine from a distance, and executed privilege elevation attacks to gain access to higher-value administrator accounts. This attack allows the hackers to hop from compromised access with a low privilege account onto accounts with much more privileges before staging the assault to extract sensitive information. Figure 6 below illustrates the process of RSA SecurID breach based on the proposed hypothesis model presented in Figure 1.

As presented in Figure 6, the proposed attack model can be utilized for attacking any type of organization. The attack process of the attackers of RSA SecurID can be well explained through the proposed attack model presented in Figure 1. By exploring the earlier research studies and based on the researchers' best knowledge, no effective research in the area of the social engineer attack process was found in a logical and detailed sequence of steps, which mimic the SE attackers' actual activities. Therefore, this paper comes to fill this gap in the literature by examining the phases in more detail.

Figure 6. Utilization of the proposed attack model for a real-life attack



## CONCLUSION

The research aims to present a new model of SE attack consists of eight phases (Identification of potential target, information aggregations, analysis and interpretation, target recognition, decision approach, armament, influence, and execution) on improved security countermeasures by considering SEI as mediating variable. The authors hypothesized the potentially mediating influence of SEI and-based on the topic of this research; this paper concluded that the new SE strategy model would present the broadest analysis of the SE attack process (Identification the potential target, target recognition, decision approach, and execution) to improved security countermeasures by considering SEI as partially mediating variable. On other hand, SE attack process (Information aggregations, analysis and interpretation, armament, and influence) to improved security countermeasures by considering SEI as fully mediating variable.

This paper has some limitations that offer opportunities for future research. The authors recognize that this study is the first step towards more practical research in the social engineer attack model. For the benefit of the research, this paper should be conducted empirically in different sectors other than Jordanian's telecommunication segment, which provides a clear picture of where attacks succeed and attempt to implement the most appropriate countermeasures. Also, the sample can be larger, which derives precise intuitions from our study. Furthermore, a larger sample size should hypothetically lead to more precise or descriptive results. Finally, the sample can include other than software development, IT support, network and infrastructure, technical operation, and other Technical employees. Furthermore, empirical research can be conducted on each one of the phases listed in the conceptual attack model, which can provide a more in-depth look at how power of influencing victims, the selection of users, and the impact of the attacks in future research would aim to retain and improve the predictive power of the model proposed in this paper. These future research can help to improve security countermeasures.

## REFERENCES

- Ahmad, S. (2017). Social engineering techniques contrast study. *International Journal of Engineering*, 9(1), 105–110.
- Albladi, S., & Weir, G. R. (2016). Vulnerability to social engineering in social network: user-centric framework. *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, 1-6. doi:10.1109/ICCCF.2016.7740435 doi:10.1109/ICCCF.2016.7740435
- Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. *European Journal of Information Systems*, 26(6), 661–687. doi:10.1057/s41303-017-0057-y doi:10.1057/s41303-017-0057-y
- Algarni, A., Xu, Y., Chan, T., & Tian, Y.-C. (2013). Social engineering in social networking sites: Affect-based model. *Internet technology and secured transactions (icitst)*, 8th international conference, 508–515.
- Allen, M. (2006). *Social engineering: A means to violate a computer system*. SANS Institute, InfoSec Reading Room.
- Brody, R. G., Brizzee, W. B., & Cano, L. (2012). Flying under the radar: Social engineering. *International Journal of Accounting and Information Management*, 20(4), 335–347. doi:10.1108/18347641211272731 doi:10.1108/18347641211272731
- Cialdini, R. (2006). *The psychology of persuasion* (revised edition). Academic Press.
- Cloppert, M. (2009). Security intelligence: Attacking the cyber kill chain. *SANS Computer Forensics*, (October), 14.
- Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, 59, 26–44. doi:10.1016/j.cose.2016.01.004 doi:10.1016/j.cose.2016.01.004
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equations models with unobservable variables and measurement error. *JMR, Journal of Marketing Research*, 18(1), 39–50. doi:10.1177/002224378101800104 doi:10.1177/002224378101800104
- Gaur, A. S., & Gaur, S. S. (2006). *Statistical methods for practice and research: A guide to data analysis using SPSS*. Sage.
- Greavu-Serban, V., & Serban, O. (2014). Social engineering a general approach. *Informações Econômicas*, 18(2), 514.
- Gulenko, I. (2013). Social against social engineering: Concept and development of a Facebook application to raise security and risk awareness. *Information Management & Computer Security*, 21(2), 91–101. doi:10.1108/IMCS-09-2012-0053 doi:10.1108/IMCS-09-2012-0053
- Hadnagy, C. (2010). *Social engineering: The art of human hacking*. John Wiley & Sons.
- Hair, J. F., Black, B., Babin, B., Anderson, R. E., & Tatham, R. L. (2009). *Multivariate data analysis* (6th ed). Upper Saddle River, NJ: Pearson Prentice Hall.
- Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, 73, 102–113. doi:10.1016/j.cose.2017.10.008 doi:10.1016/j.cose.2017.10.008
- Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare and Security Research*, 1(1), 80–91.
- Jacob, N. A. (2014). Social engineering threats in banking sector: An insight. *International Journal of Applied Services Marketing Perspectives*, 3(2), 974.
- Kanev, D. (2017). *Commitment as a constraint to the pursuit of self-interest*. Academic Press.
- Kapner, S. (2011, Oct. 31). Hackers press the ‘schmooze’ button. *The Wall Street Journal*.



- Karakasiliotis, A., Furnell, S., & Papadaki, M. (2007). An assessment of end-user vulnerability to phishing attacks. *Journal of Information Warfare*, 6(1), 17–28.
- Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 113–122.
- La Touche, P. R. (2016). The impact of information security policies on deterring social engineering attacks: The mobile worker's perspective (PhD thesis). Capella University.
- Laribee, L., Barnes, D. S., Rowe, N. C., & Martell, C. H. (2006). Analysis and defensive tools for social-engineering attacks on computer systems. *Information Assurance Workshop*, 388–389. doi:10.1109/IAW.2006.1652125 doi:10.1109/IAW.2006.1652125
- Maan, P., & Sharma, M. (2012). Social engineering: A partial technical attack. *International Journal of Computer Science Issues*, 9(2), 1694–1698.
- Medlin, B. D., Cazier, J. A., & Foulk, D. P. (2008). Analyzing the vulnerability of us hospitals to social engineering attacks: How many of your employees would share their password? *International Journal of Information Security and Privacy*, 2(3), 71–83. doi:10.4018/jisp.2008070106 doi:10.4018/jisp.2008070106
- Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. John Wiley and Sons.
- Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, 59, 186–209. doi:10.1016/j.cose.2016.03.004 doi:10.1016/j.cose.2016.03.004
- Nagy, K., Hale, B., & Strouble, D. (2010). Verify then trust: A new perspective on preventing social engineering. In *International Conference on Cyber Warfare and Security*, (p. 259). Academic Conferences International Limited.
- Oosterloo, B. (2008). Managing social engineering risk: making social engineering transparent (Master's thesis). University of Twente.
- Petty, R. E., Briñol, P., & Tormala, Z. L. (2002). Thought confidence as a determinant of persuasion: The self-validation hypothesis. *Journal of Personality and Social Psychology*, 82(5), 722–741. doi:10.1037/0022-3514.82.5.722 PubMed doi:10.1037/0022-3514.82.5.722 PMID:12003473
- Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, 11(89), 1–17.
- Sarriegi, J. M., & Gonzalez, J. J. (2008). Conceptualizing social engineering attacks through system archetypes. *International Journal of System of Systems Engineering*, 1(1-2), 111–127. doi:10.1504/IJSSE.2008.018134 doi:10.1504/IJSSE.2008.018134
- Saunders, M., Lewis, P., & Thornhill, A. (2015). *Research methods for business students*. Prentice Hall.
- Sekaran, U., & Bougie, R. (2016). *Research Methods for Business: A Skill Building Approach*. John Wiley & Sons.
- Shanmugapriya, R. (2013). A study of network security using penetration testing. In *Information Communication and Embedded Systems (ICICES)*, 2013 International Conference on, (pp. 371–374). IEEE. doi:10.1109/ICICES.2013.6508375 doi:10.1109/ICICES.2013.6508375
- Siadati, H., Nguyen, T., Gupta, P., Jakobsson, M., & Memon, N. (2017). Mind your smses: Mitigating social engineering in second factor authentication. *Computers & Security*, 65, 14–28. doi:10.1016/j.cose.2016.09.009 doi:10.1016/j.cose.2016.09.009
- Sposito, V. A., Hand, M. L., & Skarpness, B. (1983). On the efficiency of using the sample kurtosis in selecting optimal l-estimators. *Communications in Statistics. Simulation and Computation*, 12(3), 265–272. doi:10.1080/03610918308812318 doi:10.1080/03610918308812318
- Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. *Behaviour & Information Technology*, 32(10), 1014–1023. doi:10.1080/0144929X.2013.763860 doi:10.1080/0144929X.2013.763860
- Thornburgh, T. (2004). Social engineering: the dark art. In *Proceedings of the 1st annual conference on Information security curriculum development*, (pp. 133–135). ACM. doi:10.1145/1059524.1059554 doi:10.1145/1059524.1059554

Uebelacker, S., & Quiel, S. (2014). The social engineering personality framework. In *Socio-Technical Aspects in Security and Trust (STAST)*, (pp. 24–30). IEEE. doi:10.1109/STAST.2014.12 doi:10.1109/STAST.2014.12

Workman, M. (2008). Wisecrackers: A theory grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, 59(4), 662–674. doi:10.1002/asi.20779 doi:10.1002/asi.20779

Zhangbao, W., & Yang, L. (2019). On the social function of Engineering. *Procedia Manufacturing*, 30, 467–474. doi:10.1016/j.promfg.2019.02.066 doi:10.1016/j.promfg.2019.02.066

*Louay Karadsheh has a Doctorate of Management in Information Technology from Lawrence Technological University, Southfield, MI. His research interest includes Cloud Computing, Information Assurance, Knowledge Management and Risk Management. Dr.Karadsheh has published eleven articles in refereed journals and international conference proceedings and has extensive knowledge in operating system, networking and security. Dr.Karadsheh has provided technical edits/reviews for several major publishing companies, including Pearson Education and Cengage Learning. He holds CISSP, CEH, CASP, CCSK, CCE, Security+, VCA-C, VCA-DCV, SCNP, and Network +.*

*Haroun Alryalat teaching and research interest in Management Information System, E-Business and Electronic Commerce, Knowledge Management, Customer Relationship Management, Financial Information Systems, IS Project Management, IT Strategy, Enterprise Resource Planning Systems and E-Marketing. He also has an extensive experience in the assessment and accreditation processes of academic programs as well as the development of curricula for undergraduate as well as postgraduate degree programs.*

*Ja'far Alqatawna is currently a Cyber Security Researcher.*

*Samer Alhawari has received the PhD degree (2008) in Management Information Systems from Faculty of Information System and Technology, Arab Academy for Banking and Financial Sciences, Jordan. He is currently a Professor in the Department of Management Information System, The World Islamic Sciences and Education University, Jordan. His research interests include: Knowledge Management, Customer Relationship Management, Customer Knowledge Management, Risk Management, Strategic Management, Information Systems, Cloud Computing, Data mining, Text Categorization, and Project Management. Professor Alhawari has authored/co-authored over 60 research publications in peer-reviewed reputed journals, book chapters and International conference proceedings.*

*Muffleh Amin Al Jarrah is an Associate Professor in MIS, teaching at Amman Arab University.*