

# 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:

24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: [www.igi-global.com/article/the-impact-of-social-engineer-attack-phases-on-improved-security-countermeasures/286762](http://www.igi-global.com/article/the-impact-of-social-engineer-attack-phases-on-improved-security-countermeasures/286762)

## Related Content

---

### BP-Neural Network for Plate Number Recognition

Jia Wang and Wei Qi Yan (2016). *International Journal of Digital Crime and Forensics* (pp. 34-45).

[www.irma-international.org/article/bp-neural-network-for-plate-number-recognition/158900](http://www.irma-international.org/article/bp-neural-network-for-plate-number-recognition/158900)

### On the Necessity of Finding Content Before Watermark Retrieval: Active Search Strategies for Localising Watermarked Media on the Internet

Martin Steinebach and Patrick Wolf (2009). *Multimedia Forensics and Security* (pp. 106-119).

[www.irma-international.org/chapter/necessity-finding-content-before-watermark/26990](http://www.irma-international.org/chapter/necessity-finding-content-before-watermark/26990)

### Efficient Anonymous Identity-Based Broadcast Encryption without Random Oracles

Xie Li and Ren Yanli (2014). *International Journal of Digital Crime and Forensics* (pp. 40-51).

[www.irma-international.org/article/efficient-anonymous-identity-based-broadcast-encryption-without-random-oracles/120220](http://www.irma-international.org/article/efficient-anonymous-identity-based-broadcast-encryption-without-random-oracles/120220)

### Digital Forensics and the Chain of Custody to Counter Cybercrime

Andreas Mitras and Damián Zaitch (2009). *Socioeconomic and Legal Implications of Electronic Intrusion* (pp. 164-182).

[www.irma-international.org/chapter/digital-forensics-chain-custody-counter/29363](http://www.irma-international.org/chapter/digital-forensics-chain-custody-counter/29363)

### Etiology, Motives, and Crime Hubs

Debarati Halder and K. Jaishankar (2012). *Cyber Crime: Concepts, Methodologies, Tools and Applications* (pp. 1485-1498).

[www.irma-international.org/chapter/etiology-motives-crime-hubs/61022](http://www.irma-international.org/chapter/etiology-motives-crime-hubs/61022)