Taxonomy of Social Engineering Attacks: A Survey of Trends and Future Directions

Arianit Maraj¹ and William Butler²
¹Telecom of Kosovo, Technical Department, Republic of Kosovo
²Capitol Technology University, Laurel, Maryland, USA
arianit.maraj@kosovotelecom.com
whbutler@captechu.edu

Abstract: Hackers have many techniques available for breaching the security flaws of organizations. The human approach, called Social Engineering (SE), is probably the most difficult one to be dealt with. Social engineering is considered one of the most creative methods for gaining unauthorized access to information systems. This type of cyber threat does not require advanced technical knowledge because it relies mainly on human nature. Social engineers use different techniques, such as phishing, to manipulate people and cause significant damage to the organizations where they work. Therefore, organizations must raise the awareness of their users about social engineering attacks. Most organizations are putting all defense efforts into advanced technologies to prevent various threats. This is considered a wrong approach because employees of an organization use email, social networks, or other online sites as part of their work activities. Therefore, the prevention of attacks cannot be accomplished through advanced technologies alone, but the human aspect must also be studied. This paper comprehensively analyzes the existing literature in the taxonomy of social engineering attacks focusing on human aspects. It provides an overview of research opportunities that should be addressed and elaborated in future investigations.

Keywords: Social engineering, human factors, phishing, trust, perceptual, socio-emotional, education, awareness-raising, Social Engineering taxonomy

1. Introduction

With the development of new technologies, the number of devices connecting to the Internet is increasing exponentially. Today, there are approximately 46 billion Internet-connected devices (Juniper Research, 2016). With the enormous growth of devices connected to the Internet, the risk of misuse of sensitive data transmitted by these devices is increasing.

Various technologies have been developed to protect sensitive online data from cybercriminals. However, not all attacks can be detected through advanced technologies. Social engineering attacks require human interactivity, so protection against these attacks requires a different approach. Social Engineering (SE) attacks are becoming a major threat to organizations and individuals. Cybercriminals usually try to access sensitive data, such as passwords, bank account information, or access the organization's system to control the entire system (Airehrour, D. et al, 2018). These cybercriminals are using SE as a form of psychological manipulation of people into performing actions and disclosing confidential information. SE attacks are challenging to counter because they are mainly designed to manipulate human nature to disclose sensitive information online.

In general, security threats are divided into two types: technical and social engineering attacks. Technical threat means using advanced technologies to attack various individuals or organizations (Alharthi, D.N. et al., 2020, Applegate S. D., 2009). However, it has been proven that technical threats have not been effective in many cases so far. Therefore, hackers use SE techniques to bypass technical controls or advanced technologies implemented by psychologically manipulating users (Hadnagy C, 2010).

Social engineering attacks involve the psychological manipulation of users. Usually, they involve emails or other forms of communication, claiming in various false urgencies, fear, emotions, leading the victim to disclose sensitive data. Since SE involves a human element in each case, preventing these attacks is very complex, especially for organizations.

According to (Purplesec, 2021), 98% of all cyber-attacks rely on SE attacks. Therefore, it is imperative to take preventative measures to protect systems of particular importance and sensitive data. While cyber-attacks are a constant war, the only way to prevent them is to be aware of the dangers after every click on the Internet.

Through social engineering approaches, attackers can compromise many Internet-connected devices to create a Botnet (PDSC, 2020). As a result, criminals can carry out DoS (Denial of Service) (Maraj, A. et al., 2017), SQL
Arianit Maraj and William Butler

Injection (Maraj, A. et al., 2017), and attacks on various networks Lepaja, S., et al, 2018) and technologies, such as IoT (Internet of Things), Web of Things (Baraković, S., et al., 2020, Maraj, A., et al., 2019), etc.

SE attacks are becoming more common against various organizations and becoming more sophisticated. Cybercriminals are creating intelligent methods to deceive the employees of an organization, so organizations must follow proactive approaches and models to defend themselves against these attacks. Since today, individual Internet users use the Internet to perform various services, such as online shopping or other services, attackers are focusing on attacks on individuals. This paper addresses and discusses the relationships and interplay of technology, human behavior, and procedural countermeasures to protect sensitive data.

The paper is organized as follows: after the introductory section, in Section 2, we provide a theoretical background regarding the taxonomy of social engineering attacks. Section 3 describes the research methodology. Section 4 gives an overview of the existing literature addressing the impact of human factors on SE attacks. The human factors in SE and taxonomy proposal are provided in Section 5, while Section 6 concludes the paper.

2. Theoretical background

2.1 Definition of social engineering
Social engineering is one of the most creative methods to gain unauthorized access and obtain sensitive information from individuals or organizations (Alsulami, M.H., et al, 2021). SE is a collection of different techniques used to manipulate people into disclosing confidential information. The term SE is usually applied to fraud involving information collection or access to a sensitive system. In most cases, the attacker never comes face to face with the victims, and the victims rarely realize they have been manipulated (Thapar, A., 2007). Of all the information security points, people have become the weakest point. Hackers take advantage of this fact by psychologically manipulating people to persuade them to disclose sensitive information or commit malicious acts. This is why social engineering security attacks are challenging to detect and prevent (Airehrour, D., et al., 2018). To prevent SE attacks, organizations and their employees and ordinary users should be aware of the defense mechanisms that can mitigate the risk of these attacks.

Organizations mainly implement advanced technologies to detect and prevent security attacks. However, security is considered strong as the system's weakest point. According to (Schneier B., 2015), people represent the weakest link in the security chain and are responsible for the failure of a specific system. Apart from the 'human factor,' the security chain comprises technical and physical links (Kassner, M., 2020).

2.2 Social engineering categories
Social engineering attacks are classified into two main categories; non-technical attacks (human-based) and technical SE attacks (Thapar, A., 2007).

2.3 Human-based technique for hacking
Social engineering uses human behavior to exploit systems and sensitive data. In human-based attacks, the attacker interacts directly with the human target to gather the desired information (Salahdine, F. et al., 2019). Although new technologies have been used to prevent security threats, human factors have been neglected. According to some recent research, it has been discovered that today there are terms that relate to SE and go beyond technology and are based on human error and social psychology (Peltier, T.R., 2006).

Human-based attacks involve the interaction of the attacker and the victim who possesses valuable information. An SE attacker initially collects sensitive information from the target, and then through the collected information, the attackers aim to build relations with the target to gain trust. The attacker tries to persuade the victim to perform the desired actions (e.g., disclosing confidential information). The attacker uses the information gathered to carry out attacks in the final stage. Social engineering attacks are undoubtedly one of the weakest links in cybersecurity since these attacks rely on human interactions, bypassing completely technical security mechanisms (Luo X., et al., 2011).

2.4 Technical-based attacks
Through technical-based attacks, cybercriminals try to access confidential information using computer software, email attachments, and websites (Luo X., et al., 2011). In technical-based hacking, cyber attackers use advanced
techniques to gain unauthorized access. However, it is difficult for hackers to successfully attack computer systems and networks using only technical means (Applegate S. D., 2009, Alharthi, D.N et al., 2020). About 50% to 75% of cyber security threats are due to misuse of information by humans, intentionally or unintentionally (Choi M., et al., 2013). Therefore, the main focus of this paper will be on human-based attacks.

3. Research Methodology

The main goal of this paper is to contribute to SE defense methods and countermeasures. To achieve that goal, we must first understand the taxonomy of SE attacks and the role of the human factor in SE attacks. We first collected the latest literature related to SE attacks and the impact of the human factors in preventing such attacks. Afterward, we survey and compare numerous studies contributing to this field. To simplify and summarize, the main objectives to achieve the primary goal of this paper are:

- To gain a deeper understanding of the SE attacks and factors for addressing such attacks.
- To organize and synthesize the existing research literature from the field;
- To identify gaps and issues needed to be addressed by the future research activities and suggest novel and open investigation directions in the subject field.

Our research methodology relies on guidelines given by authors in (Bandara, W., et al., 2013, Levy, Y et al., 2006), Figure 1. It consists of three phases. In this manuscript, we surveyed papers coming from both the technical sciences domain and the social sciences.

![Figure 1: Research Methodology phases](image)

The first phase includes identifying and reviewing the relevant literature regarding social engineering attacks and human factors influencing SE attacks. The second phase includes the taxonomy design. The third phase includes the analysis of the selected literature and the write-up process to identify the most common SE impacting human factors. The paper will summarize how human factors can play a crucial role in increasing overall security.

4. Literature review analysis

A wide range of research focuses on technical security attacks, while fewer researchers have focused on social engineering attacks and human behavior. This section discusses research efforts related to technical and non-technical social engineering attacks.

(Ivaturi, K. et al., 2011) discussed the different types of social engineering attacks. They used the latest literature to compare and describe Social engineering methods and the factors. This manuscript presented a taxonomy approach considering human factors in social engineering attacks. The authors analyzed different types of attacks that might occur in social networking platforms, such as; person-person, person-person via media, person-person using voice, and person-person via video.

The human factors that affect social engineering attacks are considered in (Saridakis, G., et al., 2016). The authors in this paper explore how behavioral patterns impact social networks, personal characteristics, and technical efficacy of users, impacting the risk of online victimization. As human factors, they have analyzed the role of education and self-confidence in preventing SE attacks in social networking platforms, particularly in Facebook, LinkedIn, google+, and blogger. They found out that the overall intensity of social media usage alone may not increase the risk of becoming a victim of cybercrime.
Human factors impacting susceptibility to phishing attacks were studied in (Iuga, C., et al., 2016). The authors considered the relationship between demographic characteristics of individuals and their ability to detect phishing attacks and time-related factors. They gathered cursor movement data to provide additional insight. In the end, they found that gender and the years of PC usage impact the detection of phishing attacks. According to this study, many people are still at high risk of falling victim to phishing attacks. They suggest that we have to consider using a different combination of automated tools, training, and awareness-raising campaigns to prevent such attacks. The influence of demographic factors on SE attacks are also addressed in (Tynes, B.M. et al., 2014, Duggan, M., et al., 2012, and (Peltier, T. 2006).

The trust factors of social engineering attacks are discussed in (Kano, Y. et al., 2021). The authors experimented with 35 participants using pseudo-social networking service applications facing SE attacks. Trust factors are considered in (Alseadoon IMA, 2014) and (Workman M, 2007).

The authors in (Orgill, G.L., 2004) present the results of the SE audit made without any notice within one organization where data security and privacy are the primary concerns. The privacy awareness impact on SE is discussed in (Krombholz, K., 2015) and (Orgill, G.L., 2004).


The impact of human perceptual factors in social engineering attacks is considered in (Kearney, W.D. et al., 2016). According to their analysis, organizations could influence information security regarding the perception of a specific threat. User perceptions related to potential threats are also considered in (Staggs, J. et al., 2014, Vance, A., et al., 2021). Through education, training, and awareness-raising programs, user awareness can be increased (D'Arcy, J. et al., 2009).

### Table 1: Literature review analysis

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Clear aim</th>
<th>Research methodology</th>
<th>Human factors</th>
<th>Technical factors</th>
<th>Types of attacks considered</th>
<th>Platform</th>
<th>Findings</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ivaturi, K. et al., 2011</td>
<td>The papers aim is to classify social engineering attacks through taxonomy</td>
<td>The authors of this manuscript used the latest literature to compare and describe social engineering methods and the factors</td>
<td>The authors considered human factors</td>
<td>Technical factors not included</td>
<td>Person-person, person-person via media, person-person using voice, person-person via video</td>
<td>Social networking</td>
<td>The authors brought some clarity to the different types of social engineering attacks through their proposed taxonomy approach</td>
<td>This paper has a significant impact on analyzing some of the most popular SE human-based attacks.</td>
</tr>
<tr>
<td>Saridakis, G., et al., 2016</td>
<td>The authors tend to explore how behavioral patterns on social networks, personal characteristics, and the technical efficacy of users affect the risk of facing</td>
<td>Survey</td>
<td>They considered the education factor</td>
<td>Technical factors not considered</td>
<td>In general, all SE-related attacks</td>
<td>Social networking platform; Facebook, LinkedIn, google+, blogger</td>
<td>The authors of this study found that the overall intensity of social media usage may not increase the risk of becoming a victim of cybercrime.</td>
<td>This paper has some limitations, but still, it has a significant impact since it opens some future empirical work in the field.</td>
</tr>
<tr>
<td>Ref.</td>
<td>Clear aim</td>
<td>Research methodology</td>
<td>Human factors</td>
<td>Technical factors</td>
<td>Types of attacks considered</td>
<td>Platform</td>
<td>Findings</td>
<td>Impact</td>
</tr>
<tr>
<td>------</td>
<td>-----------</td>
<td>----------------------</td>
<td>---------------</td>
<td>------------------</td>
<td>-----------------------------</td>
<td>---------</td>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>Peltier, T., 2006</td>
<td>The authors examine how people, government agencies, military organizations, and companies have been duped into giving sensitive information.</td>
<td>The authors used the latest literature to compare and describe Social engineering attacks; technology and non-technology-based attacks.</td>
<td>The authors considered gender factors and education.</td>
<td>The authors considered the technology-based attacks; windows pop-ups, mail attachments, websites.</td>
<td>Impersonation, in-person</td>
<td>Internet</td>
<td>Employee education is the key</td>
<td>This paper has a significant impact on social engineering attacks</td>
</tr>
<tr>
<td>Kano, Y. et al., 2021</td>
<td>This paper explores the trust factors of Social engineering attacks on SNSs.</td>
<td>The authors experimented with 35 participants using a pseudo-social-networking-service application facing a social engineering attack.</td>
<td>Not considered</td>
<td>All SE-related attacks in Social networking services</td>
<td>Social networking services</td>
<td>They found that the profile details of the attacker and the content of the post do not affect trust.</td>
<td>This paper has a significant impact since it addresses the risks in social networks.</td>
<td></td>
</tr>
<tr>
<td>Aldawood, H. et al., 2018</td>
<td>The paper details how security education programs can increase user/employee awareness and reduce cyber security incidents.</td>
<td>Literature review</td>
<td>The authors considered the education and awareness.</td>
<td>Not considered</td>
<td>Phishing</td>
<td>Social media, jobs portals, web page</td>
<td>The authors found that implementing information security education and awareness programs can be effective to increase user awareness for preventing cyber-crimes</td>
<td>This paper is important because the authors have analyzed many recent studies in this field.</td>
</tr>
<tr>
<td>Kearney, W.D., et al., 2014</td>
<td>This study collected data from multiple sources.</td>
<td>Self-confidence and fear</td>
<td>Not considered</td>
<td>Phishing</td>
<td>Social media, Internet, Email</td>
<td>They found that as more knowledge is gained regarding how fear of providing login credentials can affect responses to phishing attacks and how self-confidence can affect the relationship between fear and intention to respond.</td>
<td>This research provides valuable information to assist in preventing the use of social engineering to obtain sensitive information.</td>
<td></td>
</tr>
</tbody>
</table>

The literature review results in this domain are depicted in Table 1. We found some important papers that address the impact of human factors in Social Engineering attacks. We selected six papers addressing human factors in different platforms, mainly on social networking platforms.
5. Impact of human factors in Social Engineering attacks and taxonomy proposal

To summarize the literature review analysis on human factors' impact on SE, several findings are depicted in Table 2. In Table 2, we selected eighteen papers that address the main human factors influencing the SE. We have noticed from this analysis that none of these papers include most of the human factors that affect SE. Therefore, this concludes that there is a need for studies that address the full range of impacting human factors in SE. Table 2 indicates that several papers address only demographic and education factors (Iuga, C. et al., 2016). Other papers address only demographic factors (Tynes, B.M. et al., 2014, Duggan, M., et al., 2012). Privacy awareness is considered by (Duggan, M. et al., 2004) and (Krombholz, K. et al., 2015). Education, Awareness raising, and Training programs are beneficial to reduce the SE risk in organizations. These factors are considered in (Iuga, C. et al., 2016, Saridakis, G., et al., 2016, Peltier, T. 2006, Luo X et al., 2011, Orgill, G.L., et al., 2004, Aldawood, H. et al., 2018). However, none of these papers (Table 2) addressed the full range of these human behavioral factors.

Table 2: Review of Human factors in Social Engineering attacks

<table>
<thead>
<tr>
<th>Ref/Human factors</th>
<th>Users demographics; Age, gender</th>
<th>Socio-emotional perspective</th>
<th>Self-confidence</th>
<th>Trust</th>
<th>Perceptual</th>
<th>Privacy awareness</th>
<th>Education/Awareness/Computer skills</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iuga, C., et al., 2016</td>
<td>✅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Saridakis, G., et al., 2016</td>
<td></td>
<td>✅</td>
<td></td>
<td></td>
<td></td>
<td>➥</td>
<td></td>
</tr>
<tr>
<td>Tynes, B.M. et al., 2014</td>
<td>✅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Duggan, M., et al., 2012</td>
<td>✅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peltier, T., 2006</td>
<td>✅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Luo X, et al., 2011</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kearney, W.D., et al., 2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alseadoon IMA, 2014</td>
<td>✅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workman M, 2007</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Staggs, J., et al., 2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Orgill, G.L., et al., 2004</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Krombholz, K., et al., 2015</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kano, Y. et al., 2021</td>
<td>✅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Orgill, G.L., et al., 2004</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aldawood, H. et al., 2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pimentel, A. et al., 2021</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kearney, W.D., et al., 2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>House, D. et al., 2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To reduce users' vulnerability to social engineering attacks, we first need to understand users' behavior and consider the impacting human factors.
The literature review revealed no previous studies investigating the full range of human impacting factors involved in human behavior. Most of the research focused on only one type of behavior. This study proposes a taxonomy, which will involve most of the human factors influencing SE attacks; users demographics, socio-emotional perspective, confidence, trust, perceptual, privacy, and education (Figure 2). We consider deficient any other analysis that does not address the full range of factors. Therefore, we think that there should be a full range of parameters.

6. Conclusions

This paper addresses and discusses the human factors which impact SE attacks. The ultimate goal is to contribute to security improvement by considering the full range of human behavioral factors on SE. The contribution of this review paper is three-fold. Firstly, we have proposed the SE taxonomy, which will address the full range of human factors impacting SE attacks. Secondly, the literature analysis and comparison have been conducted based on that taxonomy. The findings indicate that the full range of human factors have yet to be fully addressed so far. Thirdly, we have identified the gaps in human factors impacting the SE attacks. It is essential to discover how considering a full range of human factors will improve overall security, thus minimizing SE attacks and their impacts. We are convinced that the likelihood of SE attacks can be mitigated if the employees of the organizations understand their essential role in the overall strategy for SE defense. The dilemma is that organizations and their employees are at a disadvantage because they rarely face the inevitable exposure to SE attacks. Future research should focus on the least studied human factors such as Socio-emotional perspective and ones Self-confidence for example. In addition future studies should also focus on how the application of Artificial Intelligence and Machine Learning could disrupt or minimize the effects of SE attacks.

References


Maraj, A., Sutherland, C. and Butler, W., 2021, June. The Challenges to Cybersecurity Education in Developing Countries: A Case Study of Kosovo. In ECCWS 2021 20th European Conference on Cyber Warfare and Security (p. 260). Academic Conferences Inter Ltd.

Orgill, G.L., Romney, G.W., Bailey, M.G. and Orgill, P.M., 2004, October. The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. In Proceedings of the 5th conference on Information technology education (pp. 177-181).


