Cybersecurity Economics and Social Engineering: Defense mechanisms against savvy cyber-criminals

Vyshnavi Molakala Narasimhalu
5757991
Delft University of Technology
v.molakalanarasimhalu@student.tudelft.nl

***Abstract*—Despite significant advancements in security infrastructures of organizations, the incidents of cybercrimes have not reduced. Social engineering attacks have grown to be a major concern for organizations and educational institutions because humans are the bottleneck to information security. The attackers exploit human psychology to execute Social Engineering attacks. This paper focuses on applying economic theories of cybersecurity such as information asymmetry, security policies, behavioral economics to understand Social Engineering attacks and define defense mechanisms to identify and combat them. The Cialdini's principles of persuasion explain how humans can be manipulated by a social engineer. The findings show that security awareness and training programs are one of the effective defense mechanisms which can bring a shift in attitude of employees and students toward enhancing an organization's security. Moreover, additional layer of defense can be added by leveraging Artificial Intelligence and Machine Learning based systems to monitor and detect any unusual activity within an organization. Social engineering attacks are less likely to succeed when clear security policies are defined and implemented by organizations.**

I. Introduction

Even though enterprises and business firms grow diligent towards securing their infrastructures through innovative security solutions, attackers now focus on the weak link in organizations - humans. Human error is exploited by the attackers through Social Engineering (SE) techniques. SE is an art of science that defines different methods that cybercriminals exploit to manipulate people by playing with human psychology to gain access to confidential data and trick them to perform an action like transferring money to the attacker.

Phishing is one such SE technique where attackers target a person or group of people by attempting to communicate with them under false pretenses via emails, phone calls, and other means to trick them into disclosing private and sensitive information like passwords, the last four digits of credit card, etc. For instance, in 2017, Equifax was hacked for several months due to date theft of 145 million customers. Customers' personal information and credit card information were among the sensitive data stolen. The phishing attempt used to execute this breach involved sending out a large number of emails claiming to be from financial institutions or banks like Citizens Bank, Bank of America, etc [1]. According to the official statistics of the United Kingdom, the percentage of phishing attacks has increased from 76 to 86 percent in the period 2017 to 2020 [2].

If malware or viruses are how cybercriminals target computer systems and devices, SE is how they hack human minds. A recent study demonstrates that 84 percent of hackers exploit SE with high success [3]. How do the attackers successfully leverage SE? One example is the famous Nigerian Prince scam or 419 scams. A fourteen-year-old American pretended to be a Nigerian Prince and posted an advertisement in newspapers in the U.S. to send him four dollars and in exchange, the prince promised to give the people his jewels and other precious items. Many people were trapped in this scam, and they realized this fact when they did not receive the items promised by the fake prince [5]. The scammer shows a certain degree of authority by pretending to be a Nigerian prince and as a result, the victims are most likely to respond. Cialdini's "Six Principles of Persuasion" explains how people's behavior can be modified easily [6].

A cybersecurity consultant from Cyence mentioned that the United States encountered the most severe SE attacks in 2016, which resulted in a loss of 120 billion dollars. Furthermore, the U.S. FBI reported a 2.3 billion dollars loss in businesses due to a rise in fraud and email scams where cybercriminals sent emails to employees claiming to be their boss and demanding them to transfer money. These statistics illustrate the catastrophe of SE attacks and the importance of identifying and mitigating them.

The main objective of this paper is to understand how the principles of cybersecurity economics help to approach SE attacks through a new perspective. This study focuses on exploring theories of cybersecurity economics to understand the reasons for success of SE attacks, defining mechanisms to combat SE attacks and to evaluate the susceptibility to SE attack based on personality trait of an individual. The principles like behavioral economics and security policies will be discussed further in detail.

The rest of the paper is organized as follows: In Section II, some background literature highlighting the impact of the security issue and the various actors and stakeholders are described in detail. Section III describes the objective of the paper and the research questions being addressed. In Section IV, the methodology to approach the research question is discussed. Section V describes the results of the research. Further, Section VI details the limitations and future work. Finally, the conclusion and a summary of the paper are demonstrated in section VII.

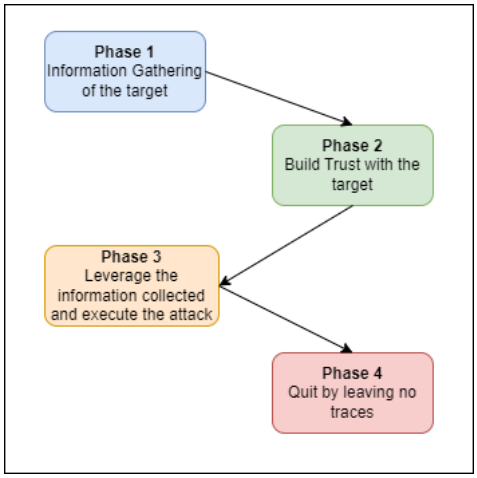

Fig. 1: Common phases of SE attacks [8]

II. BACKGROUND AND RELATED WORK

SE is presently the most serious issue, accounting for the majority of cyberattacks. Even though a threat actor's objective is to extract sensitive information like credentials or implant malware, at some point, an individual must be persuaded into acting on behalf of the threat actor. Despite the fact that new defensive mechanisms are implemented, savvy cybercriminals and threat actors continuously look forward to developing new ways to defeat these mechanisms by exploiting human behaviors and practices. In the Proofpoint Social Engineering Report of 2022, the researchers state that many malicious SE attacks were often aligned with the mistaken assumptions of the end-users [7]. One such assumption is that people believe it is safe to interact with content that comes from a source like Google, or Microsoft because they have the trust and are familiar with it.

There are various categories of SE attacks, but almost all follow a common pattern as described in the paper [8]. There are four phases: (1) Information Gathering; (2) Build Trust with the target; (3) Leverage the gathered information and executing the attack; (4) Quitting by leaving no traces. Figure 1. shows the stages of a SE attack. Phase 1 of the attack involves the attacker conducting extensive research about the target to comprehend as much information as they can. This knowledge will aid the attacker in developing rapport and trust with the target in phase 2. Once the attacker has the target's trust, he then exploits human weaknesses like persuasion, influence, and manipulation to gather additional private data, such as the target's login credentials. The attacker then leverages the information collected and executes the attack in a subtle way in phase 3. Finally, in phase 4, the attacker needs to make sure that he has not left behind any traces.

The authors of [1] give a taxonomy of SE attacks. Attackers can take advantage of physical direct communications with the target or through online means such as websites, social media platforms, etc. Phishing, tailgating, and pretexting are some of the common SE attacks exploited through direct communication with the target. Click baits on websites, fake groups and profiles on social media, SMSshing on mobiles are some examples of SE attacks through online means.

The key findings by authors in [9] are: (1) The SE attacks from 2011 to 2020 were more prevalent in financial institutions and companies, which resulted in significant economic losses due to reputational harm to the company. (2) The primary victims were the employees in the companies, people unaware of the SE knowledge, celebrities, and social media users. (3) The primary sources of attacks were emails and social media networking sites. These SE attacks are easy to conduct because the risk factor is less for the attacker.

The authors of [10] explain how cybercriminals can penetrate a secure network infrastructure by combining SE attacks with other serious attacks like man-in-the-middle attacks, exploitation of a weak credential, etc. SE attacks are a danger not just to businesses but also to educational institutions. The intensity of these attacks was evident from the scale of SE cyberattacks the educational systems witnessed during COVID-19. The statistics attributed the students' lack of knowledge about SE attacks and cyberspace to the absence of training and awareness programs conducted by educational institutions. Businesses are likely to be put in danger if students leave the educational system and enter the workforce without being aware of security issues. Hence, the authors of [11] have conducted research on the significance of collaboration between businesses and the education industry for implementing SE awareness and training programs.

The actors and stakeholders involved in the security issue are briefly described as follows: Considering SE attacks on companies, organizations, businesses, and the educational sector, the actors include: (1) Attackers are actors as well as stakeholders. They execute the attack by exploiting SE and they are stakeholders because of the economic incentives from the attack. (2) The targets of the attacker are actors because they are directly involved with the attack, and also stakeholders as they suffer losses due to the attack. (3) Companies, educational and business sectors are stakeholders because they are impacted when the targets of the attacker, either an employee or student belong to these organizations. (4) Victims of the SE attack like colleagues of the target in an organization are stakeholders because when an employee is attacked, he exposes the entire network of an organization to the attacker putting other employees at risk.

III. RESEARCH QUESTION AND OBJECTIVE

Combating SE attacks is challenging since humans are the bottleneck to security here. Human actions contribute to 82 percent of security incidents, according to the statistics from Verizon's Report 2022 [4]. It is not possible to prevent these attacks with software or hardware solutions unless people are aware of how to prevent such attacks. There are several reasons behind the motives of an attacker according to [12] such as (1) Economic incentives or profits – Cybercriminals can make profits by selling the sensitive information of the companies gained during the attack to their business competitors, (2) Revenge – This is one of the motives that drive the attackers who can either be an ex-employee or a business competitor in order to damage the reputation of the rival company, (3)

Politics - In an effort to learn vital information about their rivals or specifics about their personal lives, members of opposing political parties may attempt to carry out SE attacks. Once they have this information, they can either use it against them in a political conflict, (4) Personal interest – Sometimes attackers would carry out SE attacks purely out of intellectual curiosity about a target company, with no criminal intent.

The confidentiality, integrity, and availability of organizations will be compromised based on the severity of SE attacks. In this paper, employees of companies and educational institutions are the main targets of the attackers to exploit SE. The main objective of this paper is to use the economics of cybersecurity to approach SE attacks through a new perspective. The goal is to answer research questions (RQ) like RQ1: "Does the employees' or students' vulnerability to succumb to SE attacks depend on individuals' personality characteristics?", RQ2: "How can cybersecurity economics help us understand the reasons why SE attacks work?", RQ3: "How to define defense mechanisms to combat SE attacks?". Usually, security awareness and training programs are the basic defense mechanisms. But, according to [13], research reveals that training programs alone are insufficient to prepare employees to combat SE and suggests that multi-level layered defense mechanisms are required to effectively fight complex SE attacks. In the later sections of the paper, we can see how the principles of behavioral economics, misaligned incentives, information asymmetries, and security policies can contribute to answering the above questions.

IV. METHODOLOGY

This study is done through qualitative and theoretical approaches, where the existing secondary data from all the existing literature and various annual reports from companies and governments were used to answer the research questions. To approach RQ1, [14] and [15] were used as a reference. The authors of [14] used a theoretical approach to answer how the personality traits of an individual play a role in SE attacks. In [15], a field experiment was conducted on a private educational institution in Nairobi for a period of 14 months to collect the data to assess the vulnerability to phishing. To answer RQ2, the data collected in [16] was used. The authors of [16] collected empirical data by conducting interviews through a qualitative approach. They followed a 3-step process to collect data: (1) Planned the interview guide by choosing the target set, (2) Gathered raw empirical data by performing interviews, and (3) Perform data analysis to understand the main themes in the interviews. Some of the interviewees were security experts like Erlend Andreas Gjaere, and Mia Landsem and the victims who succumbed to SE attacks like the University of Tromso, and Cecilie Fjellhøy – A UX designer in London. For RQ3, the authors of [17] have followed an experimental approach to collect the data. Nearly 100,000 to 250,000 people living in the Netherlands were approached with the questionnaire. Some of the questions asked were: (1) Do you have any idea about the term phishing? (2) Are you aware when sharing content over the internet? (3) Are you on social media networking? (4) Have you ever succumbed to any cyber attacks over the internet or due to social engineering?

Additionally, the annual reports used were (1) United Kingdom's Cybersecurity Breaches Survey 2020 [2] presents quantitative and qualitative statistics of cyber threats and shows that majority of them are caused due to social engineering attacks such as phishing, spoofing, reverse social engineering, etc. (2) Proofpoint's 2022 Social Engineering Report [7] gives a complete overview of statistics as to why the SE attacks are successful. This was useful to approach RQ2. The reason for choosing the above cited literature and reports is that the data collected directly aligns with the research questions mentioned in this paper.

V. RESULTS

Some of the key findings of the interview conducted in [15][16] are: (1) University of Tromso suffered a loss of 1.2 million euros in 2019 due to a phishing email. The attacker successfully convinced the employee of the university to transfer the money to a different bank account. (2) Security experts tell that long term security and awareness training programs are challenging because most of the time the employees in a particular team switch companies and new members join the team. To take care of everyone in a large scale company is an arduous task. (3) Cecilie Fjellhoy was fooled by a social engineer. The attacker won the trust of the target through Tinder by pretending to like her for several months. The attacker then made up a story that he was in trouble and needed financial help. Cecilie made loans in several banks in the United Kingdom and Norway and lent the money to the attacker.

All the above examples revolve around the point that "Humans are the bottleneck to security." In the following subsection A, theories of cybersecurity economics are applied to give an explanation to the RQ1: "Does the employees' or students' vulnerability to succumb to SE attacks depend on individuals' personality characteristics?" and RQ2: "How can cybersecurity economics help us understand the reasons why SE attacks work?" and subsection B mentions about RQ3: "How to define defense mechanisms to combat SE attacks?"

A. Theories of the economics of cybersecurity

The results related to theories of the economics of cybersecurity are described in this section. The subsections present different perspectives on SE attacks. The important topics presented in this section are behavioral economics, information asymmetries, and incentives.

1) Behavioral Economics: One of the key ideas in behavioral economics is decision-making. Everyday decisions about risk and uncertainty are made by workers in organizations and students in educational institutions. A person's behavior and personality are defined by the decisions he takes. According to Kahneman and Tversky [18], the inability of people to make rational judgments is caused by the varied values they attribute to gains and losses. Heuristics are the shortcuts that people take to solve a problem quickly or to put in minimal effort. As a result, heuristics make people more susceptible to biases in their decisions. Heuristics and biases

limit rationality in the decision-making of individuals which is called Bounded Rationality. Bounded rationality is more intrapersonal i.e, an individual's susceptibility to irrational decision-making is dependent on their personality traits. A person's behavior is also impacted by the social influence and persuasion of other individuals in society on the person. The following Cialdini's Six Principles of Persuasion [19] explains how human behavior and traits make them susceptible to SE attacks.

- Reciprocity – People usually feel obliged to return favors when they receive favors from other people. For instance, scammers can build friendly relations with an employee and do him a favor by sending him a small amount of money and manipulating him to reveal his personal credentials.
- Commitment – Humans often attribute commitment and consistency to their self-reputation. Therefore, the victim continues to return favors out of commitment once the attacker is successful in persuading them to carry out a tiny action.
- Liking – People are biased towards the ones they like and are greatly influenced by them than by the people whom they do not like. Cecilie's story mentioned at the beginning of the section is an example of the degree of influence of liking on people.
- Authority – It is human nature to bow to authority. People with job titles like CEO, CTO, Senior Manager, Ph.D., or government officers wearing uniforms often make people obliged to them. An SE attacker leverages this principle and can execute the attack by pretending to be an employee's CEO or a student's professor.
- Scarcity – People are attracted to things that are scarce. Some statements like "Today is the last day to get a 50 percent discount on a hotel booking", and "Hurry up! There are many competitors to buy a house," manipulate people's behavior. Scammers can create fake scarcity and manipulate people into buying fake products.
- Social Proof – When people have limited information about a subject, they often do the same thing that others are doing. One example is pyramid schemes.

Hence, it is easier for fraudsters to deceive their targets by exploiting the above-mentioned principles to manipulate human behavior. These are one of the important reasons why SE attacks are successful. Besides, the likeliness of being attacked by SE depends on an individual's personality traits.

2) Information Asymmetries in Security Policies: Information Asymmetries occur due to imbalance in an organization when one person has better information than the other person. Security policies usually give rise to information asymmetries due to the following reasons: (1) The security-policy maker in an organization or educational institution is often more knowledgeable than employees and students. (2) The security-policy maker's lack of knowledge and awareness of the competing organizations. This will result in making poor security policies and in turn, the employees are misguided. (3) Sometimes the security policy decisions of the organizations are overly demanding resulting in a lack of proper direction for the policymakers. These asymmetries in information result in moral hazards. For instance, consider that an employee must make decisions on behalf of his manager, and both have conflicting goals. Such scenarios result in moral hazards because the employee can take more risks because the loss of such risks is attributed to organizations rather than the employee who is making the decisions. Many organizations do not want to report the statistics of security breaches due to the fear of losing their reputation and creating information asymmetries. These things also contribute to the attacker's advantage to exploit SE.

3) Incentives: Misaligned incentives of actors are again the reasons for the success of SE attacks. For instance, banks lend loans to customers easily because they have greater economic incentives. They do not consider protecting their customers from scams by making the process of granting loans harder. The attacker persuades the target to make a loan in a bank and the money goes to the attacker, and in the end, the victim is the one who suffers loss because he must repay the loan to the bank. In such scenarios, the banks have no incentives to protect their customers when they have suffered a loss due to SE attacks like scams, and phishing. The same concept applies to organizations and educational institutions. Suppose due to a lack of security awareness, an employee or a student connects an insecure device (mobile phone, laptop, etc) to the organization's Internet. This makes the Internet less secure, and all the devices connected to that network are vulnerable to cyberattacks. Furthermore, when everyone around the actor in an organization or educational institution is aware of security and acts cautiously, the cost of risk that an actor faces if he acts less securely is low. These misaligned incentives expose people in organizations to SE attacks.

B. Defense Mechanisms to combat SE attacks

This section presents the various protection mechanisms against SE attacks. These recommendations are made based on the literature and consider the human factor to prevent employees and students from being vulnerable to SE attacks. SE attacks can be exploited by direct communication with the target through daily conversations or through online means like emails, and websites. The feedback from people interviewed in [15,16] shows that the current security and training programs are not very effective. Leveraging technology and tools like Artificial Intelligence softwares to detect unusual behavior in an organization along with training programs is of the most recommended ways to combat SE attacks.

1) Improvements in Security Awareness and Training Programs: The victims of SE attacks are the ones that lack the knowledge of such attacks. The authors of [20,21] have highlighted the importance of security and awareness trainings to identify and prevent SE attacks. Usually, these security training programs occur once a year and the awareness fades away after some time. Instead of yearly programs, these

security programs must happen at regular intervals and there must be a group of people in an organization assigned to audit the effectiveness these trainings. These training programs require investment, which many firms frequently overlook. To reduce information asymmetries, these programs should be able to properly describe the organization's policies and procedures. The educational institutions must train students from all faculties and disciplines. The organizations that the students will work for in the future will be put at risk if they are unaware of these security risks. Awareness through the training programs must be especially given to the newly joined employees. Trainings must also be segregated based on the security expertise of the employees and students. For instance, an employee from non-security background would lose interest if the training program were too advanced. Similarly, an employee with security expertise would lose interest if the program were too simple. Training programs must be adaptive to the employees' personality traits. Furthermore, all the employees and students must take collective responsibility to help one another. To prevent attackers from leveraging human behavior as the weak link in SE attacks, these training programs must focus on changing employees' attitudes and building them into strong individuals.

2) Leverage Technology: Artificial Intelligence (AI) systems and softwares can be used to keep track of the emails going out of the organization, emails coming from outside organizations and report any unusual behavior. However, the continuous advancements in SE attacks can be a concern for AI based systems. But it is always good to add additional security and since these are adaptive systems, they learn and improve efficiency as time progress. Deep learning (DL) models can also be used since deep neural networks (DNN) tend to replicate human brain. Google is good in detecting spam emails. According to [22,23] DL systems play a crucial role in combating SE attacks like phishing, spam, and intrusion detection.

3) Policies: Policies are the set of procedures and rules proposed by an organization that the employees must comply with. Several researchers have mentioned the importance of well-defined policies to combat SE attacks [24,25]. Implementation of security policies guides the employees and students in identifying SE attack or an illegitimate activity. To defend SE attacks, the security policies can be divided into cybersecurity policies and communication policies. Cybersecurity policies include rules and regulations such as (1) Use multi-factor authentication, (2) Avoid using illegal softwares, (3) Connecting insecure or personal devices to organization's network, (4) Security infrastructure of organization, (5) Steps to identify an unusual activity, etc. Communication policies must be proposed since huge number of SE attacks exploit communication through emails and phone calls with the target to execute cyberattacks. A clear set of rules must be mentioned in the policy regarding internal and external communications. Policies must be defined in a way that controls the human behavior in sharing sensitive information.

VI. LIMITATIONS

The defense mechanisms to combat SE attacks mentioned in the results are very effective when they are executed in the same way as described. In reality, these theoretical solutions not always work against SE attacks. To identify and detect such attacks, relying on humans is not effective because they can be manipulated by using the theories of behavioral economics. Moreover, technological detection methods like AI, ML based systems are also not very effective since technical vulnerabilities can be exploited too. The dataset considered in this study is secondary data obtained from other literature sources. In future, own dataset can be created to assess the prevalence of SE attacks. Training youth with security awareness programs can reduce the susceptibility to attacks in future. Various other concepts of economics of cybersecurity that apply to SE attacks can be researched further.

VII. CONCLUSION

The savvy criminals take advantage of human psychology to exploit various SE attacks like phishing, baiting, pretexting, and tailgating. Even major advancements in organizational and educational security infrastructures are not able to avoid SE attacks because humans are the bottleneck to security here. Cybersecurity economic theories like asymmetric information, behavioral economics and misaligned incentives help us understand reasons for the success of SE attacks and that the susceptibility to SE attacks depends on the personality trait of an individual. In this study, various defense mechanisms like security awareness and training programs, leveraging technological advancements like AI, ML based systems to identify and detect SE attacks, and well-defined organizational and institutional security policies contribute to combat SE attacks. These defense mechanisms can result in behavior shift of the individuals and change the notion of "Humans are the weak link to security."

REFERENCES

[1] Salahdine, F., Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89.

[2] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020

[3] https://www.esecurityplanet.com/threats/fully-hackers-leverage-social-engineering-in-cyber-attacks

[4] Verizon. 2022 data breach investigation report (dbir) — Verzion https://www.veri zon.com/business/resources/reports/2022/dbir/2022-dbir-data-breach-investigations-report.pdf, 2022.

[5] Saha, B., Garcia, E., Gc, S., Li, Y. Artificial Intelligence Project.

[6] Cialdini, R. B., Cialdini, R. B. (2007). Influence: The psychology of persuasion (Vol. 55, p. 339). New York: Collins.

[7] https://www.proofpoint.com/sites/default/files/threatreports/

[8] Gallegos-Segovia, P. L., Bravo-Torres, J. F., Larios-Rosillo, V. M., Vintimilla-Tapia, P. E., Yuquilima-Albarado, I. F., Jara-Saltos, J. D. (2017, October). Social engineering as an attack vector for ransomware. In 2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON) (pp. 1-6). IEEE.

[9] Fuertes, W., Arévalo, D., Castro, J. D., Ron, M., Estrada, C. A., Andrade, R., ... Benavides, E. (2022). Impact of Social Engineering Attacks: A Literature Review. Developments and Advances in Defense and Security, 25-35.

[10] Tirfe, D., Anand, V. K. (2022). A survey on trends of two-factor authentication. In Contemporary Issues in Communication, Cloud and Big Data Analytics (pp. 285-296). Springer, Singapore.

[11] Gerow Jr, R. (2022). Social Engineering: the Need to Educate the Education Sector (Doctoral dissertation, Utica University).
[12] Zulkurnain, A. U., Hamidy, A. K. B. K., Husain, A. B., Chizari, H. (2015). Social engineering attack mitigation. International Journal of Mathematics and Computational Science, 1(4), 188-198.
[13] Gragg, D. (2003). A multi-level defense against social engineering. SANS Reading Room, 13, 1-21.
[14] Uebelacker, S., Quiel, S. (2014, July). The social engineering personality framework. In 2014 Workshop on Socio-Technical Aspects in Security and Trust (pp. 24-30). IEEE.
[15] Musuva, P., Chepken, C., Getao, K. (2019). A naturalistic methodology for assessing susceptibility to social engineering through phishing. The African Journal of Information Systems, 11(3), 2.
[16] Berg, S., Thorvik, T. (2022). Social engineering attacks in the light of security economics (Master's thesis, NTNU).
[17] Junger, M., Montoya, L., Overink, F. J. (2017). Priming and warnings are not effective to prevent social engineering attacks. Computers in human behavior, 66, 75-87.
[18] Tversky, A., Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. Science, 185(4157), 1124–1131. http://www.jstor.org/stable/1738360
[19] Cialdini, R. B. (1984). Influence: How and why people agree to things. New York: William Morrow and Company.
[20] Algarni, A., Xu, Y., Chan, T., Tian, Y. C. (2013, December). Social engineering in social networking sites: Affect-based model. In 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013) (pp. 508-515). IEEE.
[21] Smith, A., Papadaki, M., Furnell, S. M. (2013). Improving awareness of social engineering attacks. In Information Assurance and Security Education and Training (pp. 249-256). Springer, Berlin, Heidelberg.
[22] Siddiqi, M. A., Pak, W., Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. Applied Sciences, 12(12), 6042.
[23] Peng, T., Harris, I., Sawa, Y. (2018, January). Detecting phishing attacks using natural language processing and machine learning. In 2018 ieee 12th international conference on semantic computing (icsc) (pp. 300-301). IEEE.
[24] Twitchell, D. P. (2006, September). Social engineering in information assurance curricula. In Proceedings of the 3rd annual conference on Information security curriculum development (pp. 191-193).
[25] Peltier, T. R. (2006). Social engineering: Concepts and solutions. Information Security Journal, 15(5), 13.