EDU Journal of International Affairs and Research (EJIAR), ISSN: 2583-9993
Volume 5, Issue 1, January-March, 2026, Available at: https://edupublications.com/index.php/ejiar

The Role of Social Engineering in Organized Cyber Crime

Harshit Kesharwani[1], Dr. Pradeep Kumar Tiwari[2]

[1]Research Scholar, Faculty of Law, Mangalayatan University, Jabalpur, MP
[2]Associate Professor, Faculty of Law, Mangalayatan University, Jabalpur, MP

ABSTRACT

The fast development of digital technology and internet connectivity has greatly contributed to the enlargement and diversification of cybercrime activities at the global level. Social engineering, as an attack method, has gained prominence among other cyber attack modes because it is a highly deceptive tool which enables criminal hackers to take advantage of a person's weaknesses rather than finding the vulnerabilities in the entire system. Simply put, social engineering is a set of tactics that employ the art of persuasion to trick a person to give out private information like passwords, banking details, or top-secret company information. These techniques typically persuade victims through trust fear urgency, or the use of authority. The development of digital communication channels, social media, and AI has significantly increased the efficiency and complexity of these attacks. This paper reviews how social engineering is employed in organized cybercrime by first defining it, outlining common techniques, and then discussing how cybercriminal enterprises are changing their operations. The study also draws attention to the role of human vulnerability in cyber attacks and reveals the ripple effects of social engineering on individuals, companies, and government security. In addition, the paper points out the necessity of educating people on cybersecurity, having security policies in organizations, and using tech solutions to fight social engineering. It is very important to know the link between social engineering and organized cybercrime to be able to come up with good countermeasures and also to improve the overall security of the cyberspace internationally.

Keywords: Social Engineering; Organized Cyber Crime; Cybersecurity; Phishing Attacks; Human Vulnerability; Cyber Fraud; Information Security; Cybercrime Networks.

1. INTRODUCTION

The rapid growth of digital technologies, Internet connectivity, and online services has really changed the way people, businesses, and governments function. Even though these technological advances have made things more efficient and accessible, they have also opened up the possibilities for the bad guys in the cyber world to take advantage of the weak points in the digital systems. Among all the dangerous elements in today's cyber security world, social engineering is perhaps the biggest threat. It is a method that works by attacking the human factor of security instead of technical vulnerabilities. More and more, cybercriminals are using tricks based on psychology and deception to get secret information, money, or secure systems without permission. Social engineering is very important to the work of organised cybercrime, where wellplanned and coordinated actions by groups of cybercriminals are carried out to commit digital crimes[1]. Separate hackers working on their own are nothing like these organised teams of cyber criminals who, in fact, carry out their activities very much like real business entities with staff roles, lines of authority, and planned ways of working.

They use social engineering techniques to do away with normal security measures such as firewalls, encryption, and authentication by preying on human trust curiosity fear, or ignorance.The rising dependence on digital channels for banking communication shopping, and accessing government services has led to an expansion of the cybercrime environment worldwide [2]. Usually, social engineering attacks serve as an initial move in the sequence of a larger cybercrime act, allowing the perpetrators to get hold of confidential information, put malware into the system, make financial transactions fraudulently, or even take control of whole networks. To that end, one cannot underscore the importance of recognizing how social engineering and organized cybercrime relate to each other if one aims at devising viable cybersecurity measures and training programs.

1.1 Concept and Definition of Social Engineering

Social engineering is the practice of getting someone to reveal confidential or sensitive information to you by manipulating their psychology instead of computer system weaknesses. In the field of cybersecurity, social engineering is still the trickiest weapon because it affects human nature which is always the weakest part of a security chain. Cyber criminals are skilled in different methods of forking, luring, and fooling psychologically victims to get them to supply secret information like passwords, financial records, personal ID numbers, or access data. Sometimes these wrongdoers pretend to be friendly figures or institutions, like a representative of a bank, an IT person, a government official, or

even a co-worker. After the deception, they might gain the victim's confidence with which the victim is willing to give out the secret information or provide access to the closed systems, without the victim realizing it.Social engineering attacks may be perpetrated via various forms of correspondence such as emails, phone calls, use of social media sites, instant messaging apps, or even direct physical encounters [3]. Typical methods involve sending phishing emails, making scam phone calls, creating imitation web sites, and sending misleading messages aimed at instilling feelings of panic or fear. For instance, a hacker might dispatch a message stating that the target's bank account is at risk and prompt them to click on a harmful link to verify their details without delay.

1.2 Overview of Organized Cyber Crime

Organized cyber crime is about groups of people who plan and carry out crimes through the use of digital technologies in a very organized way. These groups operate in a very organized way, often resembling traditional criminal organizations, but they carry out their illegal activities in the virtual environment of cyberspace. Organized cybercrime networks are usually made up of people with very specialized skills, such as hackers, malware developers, financial fraud specialists, money launderers, and data brokers.Individual hackers might work independently for personal gain or just out of curiosity, but organized cybercrime groups have set goals, they plan strategically, and they are financially motivated. Besides, they are frequently engaged in online fraud, identity theft ransomware data breaches, financial scams, and cyber espionage. A lot of these groups operate beyond national borders, which creates great challenges for law enforcement agencies to track and prosecute offenders.

The framework of organized cybercrime networks usually features separate layers of operations. For example, some individuals may be engaged in creating malware or phishing tools, whereas others are devoted to finding potential targets and carrying out social engineering attacks. Some members may also be involved in the distribution of stolen data, illegal financial transactions, or the use of cryptocurrencies and underground markets for money laundering[4]. The rise in the complexity of cybercrime has resulted in the appearance of Cybercrime-as-a-Service (CaaS) models, where cybercriminals offer hacking tools, stolen data, and malware kits on dark web marketplaces. This change has greatly lowered the barrier to entry for cybercrime, thereby enabling even persons with limited technical knowledge to become involved in criminal activities. Usually, social engineering techniques are combined with these cybercrime operations to increase the impact of attacks.

1.3 Evolution of Social Engineering in Cybercrime

Social engineering is not a recent brainchild of tech-savvies; art of deception and manipulation have been used for ages even in the form of regular fraud schemes. Nevertheless, the emergence of digital technologies and the internet has not only increased the number of social engineering attacks but also made them more complicated and cunning[5]. Initially, social engineering in cybercrime was mostly about tricking people with simple scams like deceptive phone calls, fraudulent lottery, or impersonation to get personal information. Since the use of e-mails and other communication platforms grew rapidly at the end of the 20th century and the beginning of the 21st, cybercriminals started to back up their missions through phishing, the sending of deceitful e-mails to a large number of people for the purpose of obtaining their usernames and passwords or financial information. At that time, phishing was not highly sophisticated and hence one could easily spot it because the mails contained grammatical mistakes, suspicious links, and non-personalized texts.

Social engineering methods have indeed evolved drastically in terms of complexity and targeting capabilities. In order to execute a cyber attack that involves social engineering, today's cyber criminals do a detailed research on the victim by gathering publicly available information from social media sites, company websites and online databases[6]. These data enable the criminals to prepare very personalized fake emails, known as spear phishing, which the victim is most likely going to be convinced to open. The released technology, on the other hand, have greatly contributed to the emergence of social engineering attacks like: vishing (voice phishing), smishing (SMS phishing) and deepfake-based impersonation.

1.4 Importance of Human Vulnerability in Cyber Attacks

Human error is still the single biggest cause of successful cyber attacks despite great improvements in cybersecurity equipment and software. Besides encryption, authentication protocols, firewalls, and intrusion detection systems, security systems rely mainly on technical safeguards to protect the confidentiality, integrity, and availability of information. However, these security measures may be rendered useless if the attackers manipulate the human factor to divulge the criminals' secrets or give them unauthorized access. There are many reasons why humans are considered vulnerable to cyber threats. One factor, for example, is someone's lack of awareness of cybersecurity. Then, people just tend to trust the figures of authorities. Besides that, there are also those who act according to their emotions while others simply make wrong decisions due to cognitive biases. For example, if a person notices a message said to be from his or her boss, the person would be naturally inclined to act immediately. That is exactly what the cybercriminals count on when they first create the sense of urgency or fear in their victims' minds by sending messages threatening account suspension unless the person responds immediately. Besides that, there is another cause for human vulnerability - the digital communication platforms that have become people's main means of communication. People often get to email, social media, text, and receive notifications from different sources all the time and that makes it very

difficult to spend time stuff verifying the authenticity of each message [7]. Thus, the criminals send fraudulent messages so similar to legitimate ones, hoping that their prey will fall for the ruse.For this reason, the human factor in security must be given serious consideration if strong and efficacious cybersecurity plans are to be crafted and carried out in this age of information technology. Instilling enhanced security awareness in employees, regular staff upskilling on information security issues, and the introduction of the most stringent verification mechanisms going forward could be the best measures that companies or firms can take towards the prevention of social engineering exploits. Through sharing knowledge, raising awareness, and encouraging users to take ownership of their digital lives, both people and organizations can reach a very high level of invulnerability against cybercrimes that are planned and executed by tightly-knit criminal groups.

2. Techniques and Methods of Social Engineering Used in Cyber Crime

Social engineering is probably the most popular method in the toolkit of cybercriminals as it leverages human psychology and not the weaknesses of the technical components of computer systems. Cybercriminals know that no matter how secure a system is from a technical standpoint, it is still possible for it to be breached if someone is tricked into revealing sensitive information or giving access to the system. Therefore, attackers resort to different methods that are meant to fool, influence, or coerce the victims into actions which are secured compromised. They are diving deep into psychological triggers like curiosity fear urgency, trust, or authority to come up with such techniques.

2.1 Phishing and Spear Phishing Attacks

Phishing is one of the most common forms of social engineering used in cybercrime. It involves sending fraudulent emails, messages, or website links that appear to originate from legitimate organizations, such as banks, government agencies, online services, or corporate institutions. The primary objective of phishing attacks is to trick victims into revealing sensitive information such as usernames, passwords, banking credentials, credit card details, or personal identification information.

In a typical phishing attack, cybercriminals send mass emails to a large number of recipients with messages that create urgency or fear. For example, the email may claim that the recipient's bank account has been compromised or that immediate action is required to avoid account suspension. The message usually contains a link directing the victim to a fake website that closely resembles a legitimate one. When the victim enters their login credentials or financial information, the attackers capture the data for fraudulent use.

Spear phishing is a sophisticated and more focused form of phishing. The main difference is that traditional phishing targets the millions of people who use the Internet, but spear phishing zeroes in on a single person or a group of people within an organization. In order to do this, attackers gather their victims' information from different sources such as social media, company websites, and public records. This kind of research enables them to write very convincing messages that look real and trustworthy. For example, a hacker can send an email that looks like it came from a company's CEO asking the employee in the finance department for some confidential financial documents. Since the email looks as if it's from the CEO and is asking for something that the employee would have access to, the employee may be tricked into giving away the information. The reason spear phishing attacks are very dangerous is that they are so well crafted that the victims do not recognize them, and some times they are only detected with the help of a forensic specialist. Thus, the spear phishing method is the favorite of organized cyber criminals[8].

2.2 Pretexting and Impersonation

Pretexting is another social engineering technique in which attackers create a fabricated scenario or false identity to gain the trust of their victims. In this method, cybercriminals pretend to be someone with authority or legitimacy, such as an IT support technician, bank employee, government official, or company manager. The attacker then uses this false identity to request sensitive information from the victim.

The success of pretexting relies heavily on the credibility of the scenario presented to the victim. For example, an attacker may call an employee claiming to be from the organization's technical support team and request login credentials in order to resolve a supposed system issue. Because the request appears to come from a trusted authority, the victim may comply without verifying the legitimacy of the request.

Impersonation is a form of pretexting closely connected with it where one feigns being a trusted individual or organization to manipulate victims. Cybercriminals usually impersonate colleagues supervisors service providers, or government representatives to get confidential information. Sometimes, the attackers will make up fake email accounts, social media profiles, or websites that look almost exactly like the legitimate ones. Modern cybercrime however has also brought sophisticated impersonation methods through technologies such as voice cloning and deepfake videos. These technologies make it possible for attackers to copy the voice or appearance of real-life persons so that the fraudulent message is very convincing. These ways of doing things, which make the social engineering attacks so much easier and help the victims to be deceived without realising it, are becoming more and more popular[9]. Pretexting and impersonation attacks are more effective in companies where employees may be so used to responding to requests from their supervisors or from external service providers, that they do not question the matter. If there is a failure of a proper

verification procedure, people might be giving the information away without even realising it or giving access to the un-authorised persons to the critical systems.

2.3 Baiting and Quid Pro Quo Attacks

Baiting is a kind of social engineering technique. It is based on enticing victims with attractive or valuable items to make them lower their defense. Cybercriminals take advantage of people's curiosity and craving for rewards. They do this by offering very tempting things, for example, free software downloads movies music files, or promotional rewards. However, these offers are usually packed with malicious software that gets the user's device infected once the user accesses the file. Leaving infected USB flash drives or storage devices in public areas such as office buildings, parking lots, or university campuses is a typical baiting example. When people find these devices and connect them to their computers, they do it out of curiosity. As a result, malicious programs are automatically installed on the system. This makes it possible for the attackers to gain unauthorized access to the device or the network.

Sometimes baiting attacks in online environments are masked as advertisements or download links that offer free access to subscription-only content. Users clicking on these links may inadvertently get their machines infected with malware, spyware, or ransomware, resulting in security breaches. Another thing that a quid pro quo attack is closely related to is the trap technique whereby the attacker catch the victim by offering a service or a benefit to the victim in exchange for some sensitive information. For instance, the attackers might get hold of the victims telephone number and call them to say that they are offering free IT support service to fix a certain problem the victims system is facing and the victim in that case if he accepts the offer has to give his login credentials or be trick-to install a certain software who will grant the attackers from a distant location the possibility to have access to his computer.

2.4 Tailgating and Physical Social Engineering

Although most social engineering attacks happen in digital spaces, physical methods of social engineering still pose an imporant security risk to organizations. Tailgating, or "piggybacking, " is a method where someone unauthorized manages to enter restricted areas by following an authorized individual into a secured facility without permission. In a usual tailgating situation, the attacker may loiter around a secure door that requires IDs or access codes. When an authorized staff member comes in, the attacker courteously asks to come in with them, sometimes saying that they forgot their access card or that they are new to the company. Since people generally find it awkward to deny such requests, they might let the intruder into the building[10].

Upon entering, the attacker could get hold of personal data, classified documents, or computer systems. Physical social engineering attacks, for instance, being a maintenance man, a delivery guy, or a technician to get into limited areas. So, in order to counter tailgating and other types of physical social engineering, there need to be tight access control systems, worker understanding, and ways of checking. Workers need to be instructed to respect security rules and not to give access to people being not identified or authorized.

3. Role of Social Engineering in Organized Cyber Crime Networks

Social engineering is quite crucial for organized cybercrime networks to carry out their activities. Instead of simply trying to find and exploit software vulnerabilities like most traditional cyber attacks, social engineering aims at human nature and their inclination to trust in order to get hold of confidential information and system access illicitly. Many cybercriminal groups who are well organized frequently combine social engineering techniques with other methods so that they would be able to go around the technological security measures like firewalls encryption authentication protocols, etc.

By means of human mind manipulation into either disclosing confidential information or carrying out activities that lead to security compromise, cybercriminals can very well penetrate networks, pilfer data, and execute large-scale cyber fraud. In fact, such methods work like a charm since they take advantage not only of trust but also of other emotions like fear, urgency, and authority, which is why people are really inclined to cooperate without even asking for the legitimacy of the requests.

3.1 Social Engineering as a Tool for Financial Fraud

Financial fraud is likely the most common outcome when social engineering is used in crimes by organized cybercrime groups. Hackers usually use different tricks to lure people into revealing their bank accounts, credit cards, or other online payment details. Phishing messages, stealing information over the phone, and fraudulently imitating the websites of financial institutions are just some of the ways that scammers try to convince victims that they are dealing with legit financial institutions. In case the attackers manage to get a hold of this kind of personal information they will be able to perform unauthorized transactions, do money transfers, and carry out credit card fraud. Usually, the victims realize that they were scammed only after a great loss of money has been made.

3.2 Identity Theft and Data Breaches

One of the biggest results of social engineering in cybercrime, is identity theft. Cybercriminals are conniving their ways to steal individuals' personal information e.g. names addresses IDs, and login details. They usually do this by carrying out phishing attacks, ending people into fake registration forms, or even impersonating the person whose identity they want to steal. With the information they have, these thieves can then do all kinds of things like creating fake IDs, opening bank accounts in other people's names, or even getting into victims' financial and online services. Often these organized cybercrime groups not only store such information but also trade it on underground digital marketplaces, making identity theft a lucrative criminal endeavor.

3.3 Corporate Espionage and Insider Manipulation

Social engineering has become very popular for committing corporate espionage and manipulating insiders, for example. Hackers can try to involve company employees for them to have access to confidential business information, intellectual property, or strategic data. For instance, an attacker could pretended the company chief, IT staff or a partner that the victim was used to working with in order to be given some sensitive information or even access to a system. Also, employees may sometimes unconsciously installing malicious software or disclosing their login credentials, leading to the breach of internal networks by attackers. These kind of incidents may cause the company to loose the competitive advantages it had, suffer financially and also loosing the trust of the public in the biggest way[11].

3.4 Integration with Malware and Cyber Attacks

Today's cybercriminals are smart enough to mix social engineering and technology to get to the point. A typical phishing email, for example, will be laced with an attachment or a link that, once clicked, will download the malware to the user's computer. Monitoring of the user activity, data theft, and the granting of remote access to cybercriminals are just some of the ways this malware can be used. Cybercrime rings have exploited social engineering to carry out ransomware distribution - victims are duped into downloading programs that locked the files and demand payment to unlock them. Often these types of attacks are the work of botnets and automated systems that allow the cyber-criminals to simultaneously target thousands of victims.

4. Impact of Social Engineering on Individuals, Organizations, and Society

The extensive use of social engineering in cybercrime has serious implications for people, businesses, and society in general. Since digital technologies are penetrating more and more layers of our economic and social lives, the influence of cyber deceit has grown tremendously. Social engineering scams may result in monetary loss, invasion of privacy, mental suffering, and in some cases, the endangering of national security. To come up with efficient cybersecurity plans and precautions one must first comprehend these effects.

4.1 Financial and Economic Losses

One of the very first ways through which social engineering attacks produce an impact is by causing financial loss. Someone who gets tricked may hand over his/her money to criminals through a bank transfer done fraudulently, credit card scams, or a fraud of payment online. An organization may get losses a lot bigger from this fact considering that a data breach, taking hostage of system(s) through ransomware and business operation interruption can results in substantial changes in the bottom-line. Besides direct financial losses, other costs can arise due to gadgets recovery, insults from lawsuits and paying off the regulator. The result of these financial losses can be severe both for the company efficiency and for the general economic health stand.

4.2 Threats to Privacy and Data Security

Social engineering attacks usually lead to illegal access to both personal and organizational information. Hackers can steal or leak sensitive data like identity documents, financial information, and private business files, among others. These violations not only violate one's privacy but also pave the way for other cyber attacks like identity theft, fraud, and even spying on a competitor. Besides, data security breaches cause a loss of trust in digital systems and web services.

4.3 Psychological and Social Impacts on Victims

Besides the monetary losses, people who are tricked into giving up sensitive information might suffer a lot of psychological stress and emotional disturbance. For instance, phishing victims might feel ashamed and worried about the fact that someone obtained their private information without their consent. A company might be a victim of a security breach, which could hurt its brand and one of its main assets, customer trust. Both of these impacts, psychological for the individual and social for the institution, could certainly have lasting effects.

4.4 National Security Implications

Moreover, social engineering attacks targeting individuals and corporations can sometimes escalate to threats to a country's security. For example, cybercriminals or enemy nation agents could employ social engineering methods to get access to government bodies, military databases, or other vital infrastructure systems. Such attacks may include cyber spying, political propaganda, or causing chaos in major sectors like energy, healthcare, and transportation. Therefore, it

is no surprise that many governments across the globe are strengthening their cybersecurity strategies by incorporating measures to tackle social engineering attacks.

5. Prevention, Detection, and Mitigation Strategies

It is crucial for individuals, organizations, and governments to come up with thorough plans to prevent, detect, and respond to such social engineering attacks as they rapidly change and become more skillful. Social engineering mainly exploits human susceptibilities; therefore, a good defense strategy is a blend of awareness campaigns, security procedures of the organization, technology-based security plans, and well-established legal system. A sound multi-layered strategy is a key to lowering the risk of getting exposed to cybercriminals and keeping one's secret information from being accessed by unauthorized persons.

5.1 Cybersecurity Awareness and Education Programs

Arguably the best defense against social engineering attacks is via cybersecurity awareness and education. It is essential for individuals and employees to be able to spot the characteristic signs of social engineering between suspicious email message phone call, or request. Hence, regular training program, workshop, and simulated phishing exercises combined with other initiatives such as awareness campaign for emphasizing the need of protecting personal information, ascertaining the genuineness of requests, and reporting suspicious activities to relevant authorities or IT departments are some ways to help users acquire the skills to detect fraudulent communication and take the right steps[12].

5.2 Organizational Security Policies and Protocols

Organizations are one of the most vital elements in countering social engineering attacks. They can do this through setting up robust security policies and figuring out secure ways of operations. Besides that, the set of rules must have tough access control tools, multi-factor authentications, and proper handling of password management. Employees should be made to confirm the identity of the requesters for sensitive information or system access. Moreover, organizations should set the right rules of using confidential data and regularly update their security policies to be on the safe side against new cyber threats. Having regular audits and compliance can give more strength to the security practices of the organization.

5.3 Technological Solutions and Cyber Defense Tools

Technological defenses play an important role alongside human awareness in offering protection to systems against social engineering attacks. Highly sophisticated cyber security tools like threat detection powered by AI, technology for filtering emails, and systems designed for detecting intrusions can assist in recognizing and stopping suspicious activities before they do any damage. Programs that combat phishing, mechanisms to drastically reduce spam, and systems for detection of malware are quite efficient in keeping the source of deception and the dangerous attachments from the user's end. Besides, it is recommended that organizations frequently update their software and give them protective layers of strong encryption and security protocols.

5.4 Legal and Regulatory Frameworks

Legislative and regulatory infrastructures have a significant influence in the fight against organized cybercrime and social engineering tactics. Administrations all over the planet have implemented different sets of cyber legislation and regulations aimed at tackling issues such as online fraud, data exposure, and unauthorized entries to computer systems. These statutes define the punishments for cyber offenders and also outline the legal routes for the exploration and charging of cybercrime incidents. Furthermore, cross-border cooperation of law enforcement agencies is indispensable, considering that many cybercrime networks are operating beyond the borders of single nations. Intensifying global cybersecurity regulations and teamwork is a key factor that can lead to a marked increase in the effectiveness of combating social engineering threats.

6. CONCLUSION

It is not only the technical vulnerabilities that cyber attackers exploit, but the human factor as well. Social engineering uses various psychological tricks to manipulate and trap people into providing confidential information, giving access to the systems without authorization, and so on. Trust curiosity fear, and authority are the emotional levers these fraudsters pull to fool their victims. Various types of social engineering include phishing impersonation baiting, and physical intrusion. With the development of digital technologies and communication platforms, their execution has become tremendously advanced.The increasing reliance on digital systems for activities such as banking, chatting, and storing information has doubled the dangers of social engineering attacks. These attacks can lead to a big loss of money, stealing one's identity, disclosure of information, loss of good reputation, and even issues of national security. Therefore, dealing with problems created by social engineering must consist of awareness, security measures in organizations, technological tools, and efficient and strong laws.

7. REFERENCES

[1]. Agbaka, J. (2024). Integrated approaches to combat cyber-crime on social media: Legislative, educational, and technological solutions. *Perspektif, 13*(4), 1213–1222. https://doi.org/10.31289/perspektif.v13i4.13090
[2]. Bharati, R. K. (2024). AI-enhanced social engineering: Evolving tactics in cyber fraud and manipulation. *International Journal of Multidisciplinary Research*.
[3]. Bobokulov, A. (2023). The impact of social engineering on cybercrime: Psychological manipulation and prevention methods. *International Journal of Cyber Law*. https://doi.org/10.59022/ijcl.52
[4]. Chuquitucto Cotrina, L. K., León, P. M. S., Reyes, C. A., & Ballesteros, M. A. (2024). Cyber crimes: A systematic review of evolution, trends, and research approaches. *Journal of Educational and Social Research, 14*(5), 96–108. https://doi.org/10.36941/jesr-2024-0124
[5]. Hani, U., Sohaib, O., Khan, K., Aleidi, A., & Islam, N. (2024). Psychological profiling of hackers via machine learning toward sustainable cybersecurity. *Frontiers in Computer Science, 6*, 1381351. https://doi.org/10.3389/fcomp.2024.1381351
[6]. Naz, A., Sarwar, M., Kaleem, M., Mushtaq, M. A., & Rashid, S. (2024). A comprehensive survey on social engineering-based attacks on social networks. *International Journal of Advanced and Applied Sciences, 11*(4), 139–154. https://doi.org/10.21833/ijaas.2024.04.016
[7]. Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review, 57*, 324. https://doi.org/10.1007/s10462-024-10973-2
[8]. 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. https://doi.org/10.3390/app12126042
[9]. Chapagain, D., Kshetri, N., Aryal, B., & Dhakal, B. (2024). Deception techniques in social engineering attacks: Emerging trends and countermeasures. *arXiv preprint arXiv:2408.02092*.
[10]. Yu, J., Yu, Y., Wang, X., Lin, Y., Yang, M., Qiao, Y., & Wang, F. (2024). The shadow of fraud: The emerging danger of AI-powered social engineering and its possible cure. *arXiv preprint arXiv:2407.15912*.
[11]. Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2021). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials*.
[12]. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2022). Cyber security awareness campaigns: Why do they fail to change behaviour? *Computers & Security, 101*, 102161