Volume: 8 Issues: 50 [September, 2023] pp. 13 - 25
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.ijafb.com
DOI: 10.55573/IJAFB.085002

SOCIAL ENGINEERING AND CYBER THREATS: EXPLORING TECHNIQUES, IMPACTS AND STRATEGIES

Muhamad Baihaqi Mohd Azhar[1]
Wan Nurfitri Athirah Wan A.Azlan[2]
Wan Nursyaza Ainaa Wan Mazri[3]
Salliza Md Radzi[4] *

[1] Universiti Teknologi MARA; 2020866284@student.uitm.edu.my
ORCID ID https://orcid.org/0009-0009-2662-398X
[2] Universiti Teknologi MARA; 2020897162@student.uitm.edu.my
ORCID ID https://orcid.org/0009-0008-4544-4867
[3] Universiti Teknologi MARA; 2020834192@student.uitm.edu.my
ORCID ID https://orcid.org/0009-0002-3648-3334
[4] Universiti Teknologi MARA; salliza@uitm.edu.my
ORCID ID https://orcid.org/0009-0000-7905-6178
* Correspondence: salliza@uitm.edu.my; 0124063016.

Article history
Received date : 15-6-2023
Revised date : 16-6-2023
Accepted date : 28-7-2023
Published date : 13-9-2023

To cite this document:
Mohd Azhar, M. B., Wan A.Azlan, W. N. A., Wan Mazri, W. N. A., & Md Radzi, S. (2023). Social engineering and cyber threats: Exploring techniques, impacts and strategies. *International Journal of Accounting, Finance and Business (IJAFB)*, 8(50), 13 - 25.

Abstract: *The techniques used in social engineering, their impact on individuals, organizations, and society, and strategies against them are all covered in this article review. In order to discover and describe social engineering techniques, their effects on individuals, organizations, and society, as well as industry-adopted mitigation strategies, the study conducted a literature review using a variety of databases. The results emphasize the value of education and awareness in reducing social engineering risks. To lessen the impact of social engineering attacks, it is crucial to implement multi-factor authentication, regular system updates, clearly defined policies and procedures, and regular security audits. The importance of education and awareness in thwarting social engineering assaults, the elements of a successful training programme, and the benefits of an informed workforce are all emphasized in the essay. The first line of defence against attempts at social engineering can be a knowledgeable staff. By investing in frequent training and creating a culture of security awareness, organizations may significantly reduce the risk of social engineering attacks and secure their valuable assets.*

Keywords: *Social Engineering; Cyber Threat; Phishing.*

Volume: 8 Issues: 50 [September, 2023] pp. 13 - 25
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.ijafb.com
DOI: 10.55573/IJAFB.085002

Introduction

In the current digital era, social engineering attacks are more prevalent than ever and pose a serious threat to people, businesses, and society at large. These attacks include a number of strategies, including phishing, pretexting, and baiting, to influence people's behavior and obtain sensitive data. Social engineering attacks can have a devastating effect, leading to monetary losses, reputational harm, and psychological misery. Therefore, it is necessary to look into methods of reducing these attacks, such as awareness raising efforts, training programmes, and technology advancements. According to Sanchari, Christena, & Jean, (2020), revealed that just 13.9% of publications had user studies as their main focus. Participants in the user study were charged with differentiating between legitimate and phishing emails using scenario-based analysis. The findings indicated overconfidence regardless of the individuals' technical background, bias in self-detection was present.

This article review looks into social engineering methods, their effects on people, organizations, and society, as well as defences against them. Utilizing a variety of sources, a review of the literature was done to find and present social engineering techniques, their effects on people, organizations, and society, as well as tactics that different industries have used to combat social engineering threats.

The results of this review emphasize the value of education and awareness in reducing the risk of social engineering attacks. To provide their personnel with the knowledge and skills to identify and counter social engineering attacks, organizations must prioritize cybersecurity education and awareness. Other crucial defences against social engineering attacks include multi-factor authentication, regular system updates, carefully defined policies and procedures, and regular security audits. This article review offers insightful information about the methods, effects, and strategies associated with social engineering attacks. Individuals and organizations can better protect themselves from social engineering threats and safeguard their precious assets by being aware of the risks and putting appropriate procedures into place. According to Aldawood, & Skinner, (2019), due to the fact that social engineering assaults are created to change along with security measures and technology, more focused training is required. The knowledge base against such dangers should be expanded and improved.

Method & Material

In this study, social engineering methods like phishing, pretexting, and baiting were investigated along with their effects on people, organizations, and society through a review of the literature. Besides that, examine strategies to mitigate social engineering attacks, including awareness campaigns, training, and technological interventions. To combat threats from social engineering, a search technique based on cyber threat and social engineering was employed. The study used various databases in order to find literature that identify or present social engineering techniques, impact on individuals, organizations, and society, and strategies to mitigate social engineering attacks adopted by industries to tackle social engineering threats. The databases used are Emerald insight, Google Scholar, and IEEE Xplore. In order to find relevant literature, the search technique employed keyword patterns.

Findings

This section presents the findings of literature review regarding techniques, impacts and strategies of social engineering and cyber threat.

Volume: 8 Issues: 50 [September, 2023] pp. 13 - 25
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.ijafb.com
DOI: 10.55573/IJAFB.085002

Social Engineering Techniques

Attacks using social engineering can occur anywhere there is human contact and can take many different shapes. It is a method of communication wherein computer programmes are used to speak with individuals in order to learn information about them or exert control over them. Social engineering, as defined by Engebretson (2011), is "one of the simplest methods of gathering information about a target through the process of exploiting human weakness that is inherited by every organisation." In essence, social engineering is a deception tactic used by attackers to get beyond computer security mechanisms by taking advantage of human insiders and knowledge.

Phishing

Phishing attacks are the most common sort of social engineering attack, claim Fatima, & Naima, (2019). Through phone calls or emails, they hope to obtain private and confidential information from their intended targets. Attackers use deception to get victims to reveal private and sensitive information. They consist of fake websites, emails, ads, scareware, anti-virus software, PayPal websites, prizes, and giveaways. For instance, the attack could come in the form of a call, email, or link clicked on from a phoney lottery department asking for personal information after claiming to have won a sizable sum of money. According to Fatima, & Naima, (2019), credit card information, insurance information, complete name, physical address, pet's name, first or ideal job, mother's name, place of birth, visited areas, or any other information the individual may use to log in to sensitive accounts such as online banking or services are examples of this data. An example is an email sent to subscribers of an online service informing them of a policy violation that necessitates prompt action on their side, such as a password change. It contains a link to an illicit website that looks virtually identical to the official version, inviting the unwary user to input their existing credentials and a new password. The information is delivered to the attacker upon form submission.

Pretexting

According to Osuagwu et al., (2015), pretexting is the act of inventing and exploiting a circumstance in order to persuade a target to divulge information or allow access to sensitive documents. Answering questions unwittingly provides the attacker with all the knowledge the hacker requires to carry out the assault. According to Fatima, & Naima, (2019), pretexting assaults include the creation of fictitious and plausible circumstances in order to obtain a victim's personal information. They rely on pretexts to persuade the victim to believe and trust the offender. The attack is carried out by phone calls, emails, or physical media. To carry out their attack, attackers post information in phone books, public web sites, or conferences where collaborators in the same field gather. The pretext may be an offer to perform a service or earn a job, a request for personal information, assisting a buddy in gaining access to something, or winning the lottery. This fraud collects all kinds of relevant information and data, including social security numbers, personal addresses and phone numbers, phone records, employee vacation dates, bank records, and even security information relating to a physical plant.

Baiting

According to Kumar et al., (2019), baiting entails dangling something the user wants in order to attract the user to perform an activity that the criminal desires. It may be a music or movie download from a peer-to-peer network, or a USB flash drive with a firm logo labeled "Executive Salary Summary Q1 2013" set out for the user to locate. Then, after using or downloading the gadget, the person's or company's computer becomes infected with harmful software, allowing the criminal to progress inside your system. According to Nabie, & Paul, (2016), baiting is

Volume: 8 Issues: 50 [September, 2023] pp. 13 - 25
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.ijafb.com
DOI: 10.55573/IJAFB.085002

similar to phishing in that it uses enticement methods to seduce a victim. Hackers utilize the promise of products to entice users to give up their log-in credentials to a specific site. Baiting schemes are not restricted to digital on-line schemes. They may also be introduced via physical media. According to Fatima, & Naima, (2019), baiting attacks, sometimes known as road apples, are phishing attempts that entice users to click on a link in order to receive free goods.

Impacts of Social Engineering techniques

As one of the most common threatening attacks in the technology environment, social engineering contributes to a huge impact on the population all around the world. All of the individuals, organizations are not left behind to become targeted victims in social engineering that indirectly is giving negative impacts to them (Kumar et al., 2019). Owing to this, targeted individuals and organizations lead to giving impacts in terms of society.

Individuals

The usage of technology in the digital age where people are increasingly reliant on their devices, causes people to become unintentionally engaged or targeted in social engineering attacks. The attackers will take advantage of this opportunity and it is a bonus to them if their victims lack knowledge regarding how to secure or protect devices and the most essential is their confidential information. In other words, it is human error per omission. Other than that, the attackers also focused on specific individuals (Naumovski, & Taneski, n.d.). According to Fuertes et al., (2022), stated that new workers, middle and senior management, and famous people and politicians are a group of individuals that are usually targeted.

There are several impacts of individuals, first is confidential information has been stolen. The common confidential information that individuals have is password, credit card number, confidential documents and others. As revealed before, phishing is the most prevalent type in social engineering techniques that has been done through the Internet by sending emails that have the link were redirected to malicious websites (Aldawood, & Skinner, 2019). Generally, the emails in phishing attacks and the legitimate emails look very similar to each other. This makes it very hard to detect these attacks especially as a human that has weaknesses regarding these social engineering attacks (Joseph, 2018; Flores, & Ekstedt, 2016). According to Osuagwu et al., (2015), expressed the common email with the title of "an email to update your account". Undoubtedly, each account needs to enter the usernames as well as passwords. Once the users are deceived and believe in that, it is an achievement for the attackers. This is because as all of us know, most people reuse the same password for all of their internet accounts in order to avoid forgetting it (Naumovski & Taneski, n.d.). Thus, for sure the attackers can detect the other accounts details. As it happens to Mr. John Podesta, Hillary Clinton's campaign chairman has received emails that contain the link forged Google webpage that need him to change the passwords. He clicked on the link and changed his passwords. The perpetrator that does this is a Russian-state sponsored cyber espionage group that is known as fancy bear.

Second impact is financial losses. Nowadays, the emergence of online banking and online shopping is popular among people (Mohammad, & Gulzar, 2020). Many facilities such as the above have become an obligation in life and the use of the Internet is so high that consequences have high potential to make them vulnerable to social engineering attacks (Affan et al., 2021). Individuals will lose a significant amount of money in that circumstance. One of the studies conducted by Chitery & Singh in 2012 revealed that the financial gain through social engineering attacks is second ranked (Nabie, & Paul, 2016). Third is emotionally disturbed. Usually, in life, especially when awful incidents happen, emotions are impacted. Based on

Volume: 8 Issues: 50 [September, 2023] pp. 13 - 25
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.ijafb.com
DOI: 10.55573/IJAFB.085002

Osuagwu et al., (2015), in cases of social engineering attacks it triggers emotions of individuals that makes them feel fear, panicked, overloaded and others. It is caused by the attackers manipulating them by inducing fear or panic in them, leading them to believe that if they do not give up their information, their information will be lost (Osuagwu et al., 2015).

Organization

Indeed, every organization around the world has employees. They play a crucial part in running the organization's business so that everything runs smoothly. Depending on their position in the organization, all employees have particular access to or authority over organization information. As long as an employee has access, the organization risks becoming a victim of social engineering attempts. According to Osuagwu et. al., (2015), employees particularly those who are disgruntled or ignorant, pose a risk since they may accidentally divulge and destroy their company's secret information. Besides that, added by Naumovski, & Taneski, (n.d.), phishing email and identity theft are the major social engineering attacks that companies face. Basically, the employees will receive emails that make them believe the emails are from a higher management level in their organization or legitimate website such as job offer letters and lawyers' calls (Aldawood, & Skinner, 2019). Also, it can be through a network or system of organizations by which the attackers secretly install malicious software to get the confidential information such as financial management, assets management and control the system without being aware of the employee (Naumovski, & Taneski, n.d.). Not denied that, the information systems are very important to organizations to run their business or in other words the organization is very dependent on it (Flores, & Ekstedt, 2016). All of the above can impact organizations that lose their confidential information and financial losses. Stems from this, leads to another impact which is the reputation of the organization is decreasing due to the organization losing their customer trust or interest as well as the market share (Kumar et al., 2019; LiuXiangyu et al., 2017). The common organization that has been targeted is financial institutions that are more known as banks (Fuertes et al., 2022).

Society

Society is grouping people that live together in an organized way who share the same culture, belief and collective activities and interests. It begins with the individual where it plays a vital role in organization or a social group work, and then it develops into a society. Clearly, society has various organizations that are involved in many sectors such as healthcare, business, financial institutions, military, government agencies and others whether public or private sector where all this has contributed to the economy (Mohammad, & Gulzar, 2020; Osuagwu et al., 2015). Nevertheless, something that affects an individual or an organization will undoubtedly have an impact on society. The most significant impact is in terms of the economy where the economy in society is collapsing. Based on Fatima, & Naima, (2019), stated that companies have their own finances, if these have been attacked by social engineering where it greatly impacts the economy. For instance, the company in the United States of America, U.S. has been losing $121.22 billion since they were attacked.

Strategies for mitigating Social Engineering risks

Training and awareness

Training and awareness are two of the most effective ways for mitigating social engineering threats in today's ever-changing cybersecurity world. According to Aldawood, & Skinner, (2019) talk about the difficulties in putting social engineering training and awareness programmes into practice. They contend that conventional security solutions like firewalls and

Volume: 8 Issues: 50 [September, 2023] pp. 13 - 25
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.ijafb.com
DOI: 10.55573/IJAFB.085002

antivirus software are insufficient to defend against social engineering assaults since they are growing more complex and challenging to detect. They recommend that organisations instead concentrate on informing their staff members about the dangers of social engineering and how to recognise and counter these attacks. This paper will go through the significance of education and awareness in fighting social engineering attacks, the components of an effective training programme, and the advantages of a well-informed workforce.

Training and awareness are critical because social engineering assaults are intended to control human behavior, it is critical for individuals to recognise the signals of these attacks and respond properly. Organizations can dramatically lower the risk of successful assaults by raising awareness and teaching users about social engineering approaches. According to Aldawood, & Skinner, (2019), they admit that developing efficient training and awareness campaigns might be difficult. They point out a number of things, such as a lack of management support, a lack of resources, and employee opposition, that may prevent the effectiveness of these programmes. They also mention the necessity for training programmes to be customised to each organization's unique requirements, taking into account elements like the size of the organisation, the nature of its operations, and the technical proficiency of its staff.

Kumar et al., (2019), provide a comprehensive overview of social engineering threats and the importance of awareness in mitigating them. The authors begin by defining social engineering and its various forms, such as phishing, pretexting, and baiting. They then discuss the psychological principles behind social engineering, such as authority, urgency, and reciprocity, which are often exploited by attackers to manipulate their targets.

The use of strong passwords, two-factor authentication, and security awareness training are just a few of the steps that can be taken to fend off social engineering attacks, as the authors provide a thorough overview of all available options. They also examine the importance of technology in combating social engineering assaults, such as the usage of firewalls, antivirus software, and intrusion detection systems. Based on Kavita, Hafiza, & Nur Azaliah, (2021).

Key Elements of a Successful Training Programme

Training and awareness are critical because social engineering assaults are intended to control human behavior, it is critical for individuals to recognise the signals of these attacks and respond properly. Organizations can dramatically lower the risk of successful assaults by raising awareness and teaching users about social engineering approaches. Individuals are empowered to make educated decisions as a result of education and awareness programmes, which build a culture of security and alertness that can assist safeguard the organization from potential dangers.

Content that is comprehensive and up to date. A successful teaching and awareness programme should include phishing, pretexting, baiting, quid pro quo, and tailgating, among other social engineering strategies. The content should be updated on a regular basis to meet emerging dangers and attacker techniques.

Examples and simulations from real life. Real-world examples and simulations incorporated into training materials can assist users in better understanding the risks and repercussions of social engineering attacks. For example, simulated phishing exercises can provide useful information into how users respond to phishing emails and help identify areas for development.

Volume: 8 Issues: 50 [September, 2023] pp. 13 - 25
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.ijafb.com
DOI: 10.55573/IJAFB.085002

Methods of instruction that are interactive and interesting. Organizations should employ interactive and engaging training approaches to maximize the success of education and awareness programmes. Gamification, role-playing exercises, and group discussions can all help users remember material and apply it in real-life circumstances.

Lastly Aldawood, & Skinner, (2019), offers insightful information about the difficulties in executing training and awareness campaigns that focus on social engineering in cyber security. Their analysis emphasises how crucial it is to address cyber security holistically, with not only technical safeguards but also personnel education and awareness campaigns.

The Advantages of a Well-Informed Workforce

A knowledgeable staff can be the first line of defense against social engineering attempts. Employees can assist prevent data breaches, financial losses, and brand damage by recognising and reporting suspicious activity. Security awareness culture can contribute to a more resilient organization that is better able to adapt to an ever-changing threat scenario. Furthermore, organizations that prioritize cybersecurity education and awareness are more likely to attract and keep top talent, as employees increasingly respect companies that prioritize security.

Use multi-factor authentication (MFA)

Implementing strong security measures becomes more crucial as social engineering assaults continue to pose serious hazards to people and organisations. Multi-factor authentication (MFA) is one such mechanism that adds an additional layer of security by forcing users to give additional verification in addition to a straightforward username and password. According to Arora, & Jain, (2021) do a bibliometric analysis of the literature on cyber security threats and their deep learning-based countermeasures. They note a number of significant trends in the literature, such as an increase in interest in employing deep learning techniques to identify and stop cyberattacks and an emphasis on creating more potent defences against certain threats, such malware and phishing.

Multi-factor authentication (MFA) is one approach that is commonly cited in the literature. Users must present two or more forms of identity in order to access a system or application when using MFA as a security mechanism. This can be something that the user has (like a security token), something that the user knows (like a password), or something that the user is (like a fingerprint or facial recognition). MFA, according to Arora, & Jain, (2021), makes it far more difficult for attackers to access systems and applications, even if they have the user's password. This makes it an effective technique to prevent unauthorised access to systems and applications. They also note that MFA is becoming more significant as more businesses switch to cloud-based programmes and services that can be accessed from any location in the world.

Benefits of Multi-Factor Authentication

Enhanced security:
By requiring additional authentication, MFA considerably lowers the danger of unauthorized access. As a result, even if an attacker has access to a user's password or other credentials, they will have a harder time compromising account.

Protection against social engineering attacks:
By imposing extra authentication elements that are challenging for attackers to obtain or duplicate, MFA might help lessen the effect of social engineering assaults like phishing.

Volume: 8 Issues: 50 [September, 2023] pp. 13 - 25
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.ijafb.com
DOI: 10.55573/IJAFB.085002

Compliance with industry regulations:
MFA implementation is mandated in several sectors, including banking and healthcare, in order to safeguard sensitive data and adhere to legal requirements.

Improved user experience:
Modern authentication techniques, including biometrics and push alerts, may offer a smooth and user-friendly experience even if MFA may at first appear to be onerous.

Update and patch systems on a regular basis

Attackers are continually finding and using system vulnerabilities in the digital environment of today. Establishing comprehensive vulnerability management programmes that include routine system upgrades and patching is crucial for organisations if they want to reduce risks. This essay will go over the value of patching and updating systems, the repercussions of doing otherwise, and the ideal procedures for a successful vulnerability management approach. According to Osuagwu et al., (2015), discuss the importance of mitigating social engineering attacks for improved cybersecurity. They argue that social engineering attacks are becoming increasingly common and sophisticated, and that organizations need to take proactive measures to protect against them.

Osuagwu et al., (2015), also acknowledge that updating and patching systems can be challenging, particularly for large organizations with complex IT infrastructures. They suggest that organizations need to develop clear policies and procedures for managing updates and patches, and that they need to prioritize critical systems and applications to ensure that they are updated in a timely manner.

The Need for Continual Patching and Updates

Systems and software both include flaws that attackers can use to compromise systems or gain unauthorised access. Updates and patches are often released by vendors to fix newly identified security flaws and vulnerabilities. However, organisations frequently neglect to apply patches and upgrades when they become available, leaving their systems open to attack. Systems can be updated and patched often by organisations to:

Reduce vulnerabilities:
Updates and patches include security fixes for flaws that hackers may try to exploit. Installing them reduces risks and guards against system compromise.

Improve functionality:
Updates frequently include improvements and brand-new features that enhance the performance, usability, and usefulness of software and systems.

Ensure compliance:
Businesses must install security updates and patches in a timely manner in accordance with numerous industry laws and standards. If you don't, you risk legal repercussions and reputational harm.

Clearly define policies and procedures

Attacks using social engineering take advantage of human weaknesses to obtain unauthorised access to confidential data or systems. Organisations must create clear policies and procedures that instruct employees on how to handle sensitive information, report problems, and gain

Volume: 8 Issues: 50 [September, 2023] pp. 13 - 25
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.ijafb.com
DOI: 10.55573/IJAFB.085002

access to systems in order to effectively manage these dangers. The significance of clearly stated policies and processes, essential components to have, and the advantages of an organised approach to addressing social engineering risks are covered in this essay. According to Aldawood, & Skinner, (2019), is clearly defining policies and procedures for managing cyber security risks. They note that policies and procedures should be tailored to the specific needs of each organization, taking into account factors such as the size of the organization, the nature of its business, and the level of technical expertise of its employees. They also suggest that policies and procedures should be regularly reviewed and updated to ensure that they remain effective in the face of evolving threats.

The importance of using a range of tools and applications to protect against social engineering attacks. These can include everything from firewalls and antivirus software to more advanced tools such as intrusion detection systems and security information and event management (SIEM) systems. Based on Aldawood, & Skinner, (2019).

The Importance of Clear Policies and Procedures

The security posture of an organisation is built on clear rules and processes. They assist prevent unintentional behaviours that could result in security incidents by giving employees a clear awareness of their duties and expectations. Organisations can: By adopting and upholding policies and procedures, they can:

Reduce human error:
Employees may handle sensitive information more safely and prevent behaviours that could expose the company to social engineering assaults with the help of clear standards.

Promote a security-aware culture:
Employees are more likely to identify and report potential threats when there is a culture of security awareness, which is helped by policies and procedures.

Promote a security-aware culture:
Security gaps are less likely to occur thanks to standardised processes that make sure all staff follow the same security procedures.

Ensure consistent practices:
Organisations can promptly address possible dangers and minimise harm when reporting and responding to occurrences according to well-defined protocols.

Perform routine security audits

Risks associated with cybersecurity are always changing in the current threat scenario. Organisations must conduct regular security audits and assessments to understand their security posture, address weaknesses, and fortify their defences against possible threats. This essay will examine the significance of performing regular security assessments, the essential elements of a successful review, and the advantages of continual observation and development. According to Krishna, (2023), cyber security audit is essentially defined as a procedure involving a detailed assessment and analysis of the IT infrastructure of a company. It is a key method to check compliance and plays a significant role in discovering threats and vulnerabilities, displaying weak linkages, and other high-risk practices. Through the gathering of secondary data, this study intends to investigate the role performed by cyber security audits in the management of cyber security risks with regard to business systems and applications.

Volume: 8 Issues: 50 [September, 2023] pp. 13 - 25
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.ijafb.com
DOI: 10.55573/IJAFB.085002

The Need for Continuous Security Evaluations

Every day, new cyberthreats materialise, and hackers are continually coming up with new ways to attack systems and data. Organisations may better understand their existing security posture, find exploitable vulnerabilities, and manage risks by conducting regular security audits and assessments before bad actors can exploit them.

Conducting regular security evaluations is important for a number of reasons, including:

Identifying vulnerabilities:
System, software, and process vulnerabilities that may be used by attackers are found during audits and assessments. Taking care of these weaknesses lowers risks.

Ensuring compliance:
Organisations are required by many industry requirements to regularly conduct security audits and risk assessments. Constant assessments aid in demonstrating compliance and avoiding potential sanctions.

Improving security controls:
The effectiveness of a company's security controls and procedures can be learned from audits. To enhance defences and make changes, use this knowledge.

Minimizing threats:
Organisations can lessen opportunities for threats to materialise and avert potential assaults by proactively recognising and reducing risks. A state of continuous security monitoring and risk minimization is achieved with the aid of regular audits.

Discussion

Based on the findings, social engineering techniques are used to manipulate the behaviour of a target audience. These techniques include using a combination of various methods such as telephone, email and direct mall. Phishing is one of the techniques which has been used for many years. It is a form of spam that uses computer programs to trick a user into sending an email with a link to another website. Phishing is a type of malicious program that attempts to get users' personal information. The purpose of this attack is to steal. This is done through various means such as using cookies, which are used to identify people who have personal data and then sell it to other companies. Next is pretexting which is a method of spreading messages by sending text messages to people. These messages are sent to people's phones, and they can be read by anyone on the internet. This technique is very effective because it allows the person to send messages without any thought or hesitation. Lastly, baiting is another type of social engineering that involves using words to get people's attention. It is used to lure people into clicking links or sharing information about products. It is a form of social engineering which uses the power of persuasion to persuade people into purchasing something. This method is used by companies to gain their customers' trust.

Apart from that, social engineering attacks impact individuals and organizations where attackers have targeted both. Obviously, this is due to the individual and the organization itself. This has been proven the cause of social engineering attacks. Among them are the lack of qualified human resources, human error every time, personal interaction in social networks, perception of human behaviour, overconfidence, lack of protection in the system and ineffective hardware and software defences. Not enough with that, the phishing techniques have given

Volume: 8 Issues: 50 [September, 2023] pp. 13 - 25
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.ijafb.com
DOI: 10.55573/IJAFB.085002

highly impacts to individuals, organization and society. With the causes that come from the individuals and organization, they are unable to recognize the phishing emails. Furthermore, 85 percent of companies have been attacked by phishing techniques at least once. Then in 2020, the data breaches that involve phishing as much as 22 percent (Fuertes et al., 2022). This can be viewed as the phishing is successful in social engineering attacks. Based on the findings of the impacts above, the majority impact that has impacted all individuals, organizations and society is in terms of financial. However, the impact of financial losses will not occur if the attackers do not successfully steal the confidential information of individuals or organizations. Thus, the confidential information has been stolen and financial losses have links to each other. To sum up, the financial impact is a key indicator of social engineering impacts for both individuals and organizations and as a cause of cyber theft (Nabie, & Paul, 2016).

Strategies to lessen the risks posed by social engineering attacks, which are constantly evolving and provide serious challenges to organisations. Effective protection requires a multifaceted strategy that incorporates security training and awareness, technical controls like MFA, routine updates and patching, unambiguous policies and processes, and regular security audits. As social engineering attacks frequently rely on tricking users into disclosing sensitive information or doing activities that jeopardise security, education and awareness are essential to preventing them. Organisations can lower the likelihood of successful assaults by teaching staff and users to spot and report social engineering attempts. Another important tactic is to use MFA, which adds an additional layer of security and can assist prevent unauthorised access. By requesting consumers to produce further proof of identity. Another important tactic is to use MFA, which adds an additional layer of security and can assist prevent unauthorised access. MFA can aid in preventing attacks that rely on stolen or compromised credentials by forcing users to give additional verification in addition to a password. System updates and patches must be applied on a regular basis since software and system flaws can be used by attackers to compromise systems or gain unauthorised access. Organisations can reduce the risk of successful attacks by maintaining updated software and systems.

Conclusion

Overall, this paper attempts to provide a comprehensive overview after the literature review is implemented related to social engineering and cyber theft in terms of techniques, impacts, and strategies. As previously revealed, social engineering techniques include phishing, pretexting, and baiting. This is followed by how it impacts the individual, the organization, and society with the financial losses being the major impact. To address these, strategies play critical roles which are a solution in mitigating social engineering attacks. For example, an awareness campaign. As a result, this study is significant since it exposes all people throughout the world to social engineering and cyber threats with the intention of raising knowledge about it. The spread of this gives a great knowledge base about this as well as the cybersecurity to everyone from children to adults. This is due to the fact that, causes of social engineering attacks coming from the individuals and organization such as human behaviour, human error per omission. It also can be claimed that there is a lack of knowledge about these. Moreover, as we all know day by day social engineering attacks are growing rapidly worldwide. If it is not prevented, it will get worse with widespread impacts than existing. Therefore, this paper bestows a clear understanding of the precise concept of social engineering and cyber threats.

Volume: 8 Issues: 50 [September, 2023] pp. 13 - 25
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.ijafb.com
DOI: 10.55573/IJAFB.085002

Acknowledgments
In this section, you can acknowledge any support given to the project. We thank Muhamad Baihaqi Mohd Azhar, Wan Nurfitri Athirah Wan A.Azlan and Wan Nursyaza Ainaa Wan Mazri for useful discussion. We thank Madam Salliza Md Radzi for the support.

References

Affan Yasin, Rubia Fatima, Liu, L., & et al. (2021). Counteracting social engineering attacks. *Computer fraud & Security, 2021*(10), 15-19. https://doi.org/10.1016/S1361-3723(21)00108-1

Aldawood, H., & Skinner, G. (2019). Challenges of implementing training and awareness programs targeting cyber security social engineering. *2019 cybersecurity and cyberforensics conference (ccc)*. 111-117. DOI 10.1109/CCC.2019.00004.

Aldawood, H., & Skinner, G. (2019). Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal. *International Journal of Security (IJS), 10*(1).

Arora, P., & Jain, A. (2021). Cyber Security Threats And Their Solutions Through Deep Learning: A Bibliometric Analysis. *Journal of Information Security and Applications 60*, 102778. doi: 10.1109/ICAC3N53548.2021.9725480

Das, S., Nippert-Eng, C., & Camp, L. J. (2022). Evaluating user susceptibility to phishing attacks. Information & Computer Security, 30(1), 1-18.

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *59*, 26-44. https://doi.org/10.1016/j.cose.2016.01.004

Fuertes, W., et al., (2022). Impact of Social Engineering Attacks: A Literature Review. *Development and Advances in Defense and Security*. https:// doi.org/10.1007/978-981-16-4884-7_3

Galinec, D. (2023). Cyber Security and cyber defense: Challenges and building of Cyber Resilience Conceptual Model. *International Journal of Applied Sciences & Development*, 1, 83–88. https://doi.org/10.37394/232029.2022.1.10

Jadhav, K. D. (2023). The Role of Cyber Security Audits in Managing Company Systems and Applications. International Journal of Computer Science and Mobile Computing, 8(6), 1-6.

Joseph, M. H. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computer and Security, 73*, 102-113. https://doi.org/10.1016/j.cose.2017.10.008

Lee, Y. Y., Gan, C. L., & Liew, T. W. (2022). Phishing victimization among Malaysian young adults: cyber routine activities theory and attitude in information sharing online. The Journal of Adult Protection, (ahead-of-print).

LiuXiangyu, LiQiuyang, & Chandel, S. (2017). Social engineering and Insider threats. *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*. DOI 10.1109/CyberC.2017.91

Lohani, S. (2019). Social engineering: Hacking into humans. *International Journal of Advanced Studies of Scientific Research, 4*(1).

Mohammad Hijji, & Gulzar Alam. (2020). A multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the Covid-19 Pandemic: Challenges and Prospective Solutions. *Digital Object Identifier, 9*. 10.1109/ACCESS.2020.3048839

Nabie, Y.C., & Paul, J. S. (2016). Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research, 6*(23). http://dx.doi.org/ 10.19101/IJACR.2016.623006

Naumovski, T., & Taneski, N. (n.d.). Social Engineering in the Context of Cyber Security.

Volume: 8 Issues: 50 [September, 2023] pp. 13 - 25
International Journal of Accounting, Finance and Business (IJAFB)
eISSN: 0128-1844
Journal website: www.ijafb.com
DOI: 10.55573/IJAFB.085002

Osuagwu, E. U., Chukwudebe, G. A., Salihu, T., & Chukwudebe, V. N. (2015). Mitigating social engineering for improved cybersecurity. *International Conference on Cyberspace Governance (Cyber-Abuja)*. 91-100.

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet, 11*(89), 1-17. doi:10.3390/fi11040089

Sekaran, K., Hafiza Abas., & Nur Azaliah Abu Bakar. (2021). A Study of Social Engineering: Threats, Awareness and Measures. *Razak Faculty of Technology and Informatics*, 10(7), 1-7. doi: n.a

Xu, T., & Rajivan, P. (2023). Determining psycholinguistic features of deception in phishing messages. Information & Computer Security, 31(2), 199-220.

Yerima, S. Y., & Alzaylaee, M. K. (2020). High accuracy phishing detection based on Convolutional Neural Networks. *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS).* https://doi.org/10.1109/iccais48893.2020.9096869