BSc (Hons) in Information Technology Specialized in Cyber Security

Sri Lanka Institute of Information Technology

Introduction to Cyber Security (ICS):

Social Engineering and phishing attack

MNM. RUHAIM

IT23256446

Contents

ABSTRACT

Now a days the development of digital technology and the development of of the social media network and made the communication of human beings between each other more easily, but we are share the personal information and private information and the participation of others via the Internet, it is a more danger. that this information can be exploited and collected, and from this a new methord called as a social engineering. Social engineering has expand that is the attackers wants Damage to people searches and collects personal and confidential information to penetrate and cause harm to the victim. The phishing is the most popular and most common threats attack in social engineering that the people facing most dangers attack. Moreover, this report will be discuss how to Survey Techniques to make secure from this type attack and try to increase the awareness of defense and increase human culture from Being caught in a phishing scam or phishing attack. These attacks aim to trick individuals or companies into carrying out actions that benefit the attackers or provide them with sensitive data via e-mail messages or malicious and fake software that shown as a real site and asks them to do so. such as credit card and passwords. Social engineering is one of the biggest challenges to network security because it takes advantage of the natural human tendency to trust. In conclusion, Recommend Some Preventive Measures and Possible Solutions to the Threats and Weaknesses of Social Engineering. In this report, gives the summarizes the concept of social engineering and how the attacker seeks For that, it starts with attack, phishing, It is a mixture of social engineering and technical methods to persuade the user to disclose his sensitive and personal data, in addition to phishing classifications via social engineering.

INTRODUCTION TO THE SOCIAL ENGINEERING AND PHISHING ATTACK

Modern cybersecurity faces numerous threats, especially in the digital environment, as it rapidly develops. social engineering attacks. These attacks capitalize on human factors considered to be the main weak link in. security measures, through coercion to reveal crucial information from people. Among the most the best known type of social engineering is phishing, in which criminals employ trickery—most often through emails or scams to lure the victims into providing their login information to fake websites. This strategy also affects personal: The above tactics not only undermines personal: and organizational data as well greatly affects the psychological health of the targeted individuals. With the advance in the use of digital communications and the social media, it has become easy for invaders to implements phishing attacks, thus moving beyond solution like firewalls and antivirus programs. As these attacks as they have turned more frequent and intelligent, they have proved to be the greatest danger to cybersecurity. at the same time, such networks work irrespective of the existing technological protection in an organization. To minimize the impacts of phishing as well as other social engineering techniques, there is need to That is why some organizations have had to put in place security measures, which include training their employees on security measures. Raising awareness, a set of measures aimed at increasing the level of awareness among the company's employees about the features of phishing and providing them with knowledge of how to respond can be process efficiently has become a necessity when it comes to protecting organizational data and system continuity. This report will review the trends of applied approaches to phishing attack and other types of social engineering threats in different industries. emphasizing the need to strengthen the approach to information security awareness as a countermeasure against cybercrime.

What is social engineering

Social engineering is a strategy that tries to take advantage of the people's psychology to ensure they reveal details or data, or grant access to the attacker. Traditional cyberattacks involve a weakness of the cyber security system of a company and organization apart from manipulating the system, it is a kind of cyber attack that exploits the human being.

Social engineering in its essence is a manipulation process that most often entails the use of force, primarily human emotions such as fear, haste or trust. Some of them are as follows; phishing that is false emails and text that are made to look genuine, with an aim of getting the users to divulge their personal information. Pretexting involves seeing the target into a scenario that is false, but real enough that the target will provide information willingly to. Baiting involves deceiving the target with promises of a reward with gifts like free downloadable items then introducing the malware.

The advances in digital communication, social networks as well as the possibilities of e-Crime and fraud have opened many ways for social engineering attacks when hackers gather personal data and subsequently train to make proper contacts of chosen individuals or different organizations. This sort of targeting makes it easier for the attacker to design a narrative that would appeal to the interest or association of the victim.

Reducing the risks of social engineering calls for a two-pronged approach comprising of sensitization and appropriate measures towards protection. It becomes the responsibility of organizations to ensure that the employees of the organization undergo several trainings with a view of identifying the existing threats and what can be done regarding the threats. By training people to be more observant and critical, the general public and particular companies and organizations can minimize their vulnerability to new types of social engineering threats.

Social Engineering Attacks

Social engineering is the art of deception through which the attackers have to communicate with the target and get him or her to do something which is dangerous to the security of the company. These attacks do not necessarily take advantage of any programming or mechanical loopholes but instead depend of tricks that human emotions are bound to fall for.

The type of social engineering attack seen most often is phishing. In phishing, an attacker sends a spam mail, which looks like it has originated from a genuine organization like a bank or even a reputable online service provider. The email can have a slight touch of the urgent, forcing the recipient to attend to a link that is a trap or type in her or his secret information. For instance, a victim might get an email note that his or her bank account will be locked if one does not provide the account details promptly. Such urgency is likely to result in making wrong decisions and increasing the level of insecurity.

Other one is pretexting where the attacker sets up an incident for obtaining information of his/her choice. For instance, a hacker poses as an official from the employee's company and calls the employee, pretending to be from the IT department in order to confirm login details to update the company's integrated system. Fiduciary of the caller, the employee is likely to share some information without regard.

Mishandling is another method in which the attackers try to trick or entice the victims in a given network. A primary example they give includes placing infected USB in certain area s of the public with the hope that someone will insert the affected USB onto the respective computer.

Social engineering attacks can also be through social media where a person gathers personal information to develop a good story to use for deception. For example, they may investigate a person's relationships and hobbies in order to craft the message they send as part of phishing.

In response to these threats, people and organizations need to take proactive approach within the community by ensuring everyone becomes aware of the threats and invest adequate time into training people how to be wary of any unexpected messages and be extremely careful in any online interactions.

Phishing attacks

Phishing is a type of cyber criminal activity where people are deceived into divulging personal information, including user names, passwords, credit card numbers, and other types of data. This is usually done form a face recognizable as that of a well known entity for instance an email message that appears to be from of a legitimate institution.

In a standard phishing scheme, the attacker sends an email with an appearance that it came from a trustworthy entity like a bank, social networking site, or service provider. The email is usually written in an alert tone, including notifications about accounts, or security concerns, that require a response with immediate action. This can range from joining a link that takes the user to a fake and look like like the original site. Once the victims are there they may be required to type their login details or any other information and this is well recorded by the attacker.

They can also be categories into more complex types like the spear phishing which are usually in specific individuals or companies. These attackers make the deception a lot better since they post the personalized information on social media or obtain it from other sources. For example, a spear phishing email could mistakenly read as though it was from a co-worker who worked with the individual in a prior company project.

Another variation is whaling, in which the targeted are selected according to their responsibilities and job titles that the attacker wants to use in some way.

The implications of becoming an affiliate of the phishing attacks can often have very dire consequences such as, loss of money, identity theft as well as having the accounts one uses become breached. However, to avoid or reduce such risks, people and organizations require to be more cautious. Frequent training in how to avoid phishing scams, how to use multiple factors identification, and keeping the security programs updated considerably minimizes the chances of becoming a victim of these scams.

INFORMATION SECURITY AWARENESS IN A SOCIAL ENGINEERING

Information security awareness is an essential component of organizations' information security. Employees are important organizational assets because of their capability to make crucial information security decisions when the need arises. Information security awareness programs can support and develop such capabilities. In this paper, information security awareness is defined as ensuring that all members in an organization understand their roles in protecting data and information. Organizations need to verify that all staff know their roles and responsibilities in safeguarding the information that is in their possession.

Computer technical attacks differ from social engineering attacks based on the technical level of personnel involved in the security breach. Common technical attacks would most likely involve staff from IT departments, which probably have in house experts with security and technical knowledge to handle it. However, social engineering attacks target all levels in organizations, from cleaners who work after regular working hours up through executives. Targeted personnel might have insufficient technical experience or may be unaware of social engineering concerns. For example, a large number of employees do not know the exact classification of information in their possession. It is practically impossible to eliminate social engineering breaches without working on improving the level of information security awareness among all staff.

A multilayered approach with a combination of technical security and increasing the information security awareness level of members, is necessary in order to build a great defense against social engineering attacks.Literature suggests implementing and introducing information security awareness programs to protect the firewall composed of the human mind against social engineering strategies. Mouton et al in for example, listed some recommendations to reduce the risks related to various social engineering attacks. They argue that there is a necessity for organizations to provide educational training for every single employee to help them establish an information security culture in the workplace and make employees aware of the different methods used or followed by attackers. Similarly, notes the need to underline the security of a person's information security awareness within the whole organization to avoid a possible leakage of any confidential data. Furthermore, other studies like confirm that as long as staffs are not conscious and aware of possible threats caused by social engineering, technical measures are insufficient. In terms of the individual awareness level on social engineering threats, several studies have highlighted users' lack of understanding of security and privacy threats associated with personal smart devices they tend to use. For instance, it is noted in literature that users of various technological e-health devices are not aware enough of the latest threats and social engineering techniques that can take advantage of their shared personal data. Additional human factors were also studied by Billikens et al. in which they collected survey data from students and professionals in various universities across the United States to investigate the privacy and security risk

associated with social engineering in personal e-health services. Those who participated in the survey showed very poor understanding along with a lack of knowledge regarding the technologies they elected to use. As a result, researchers argue that new security and confidentiality actions should be developed with an emphasis on improving the user overall threat awareness caused by similar smart devices. Human aspects are major factors in safeguarding information properties that could be sources of harms to the overall safety of an establishment. Trust is among the leading security elements that is associated with human's nature.

Researchers argue that trust is vital in every aspect of an information security system and may affect security conduct considerably. For instance, is a trust survey indicating that most computer users lack security awareness and tend to be overly trusting of strangers. This study, like many others, concluded that when computer users are aware of the risks surrounding them and the signs of a potential threat, self-security against trust can be significantly improved. The training of staff enables them to effectively adhere to sound cyber security practices. Hence, awareness and training programs complement each other, influencing users to develop their security behavior for managing possible cyber-attacks

EVOLUTION OF THE SOCIAL ENGINEERING AND PHISHING

1. **Pretexting:** This works entails the development of a scenario, in which a subject is deceived, in order to gather certain information. An attacker might pretend they are an employee or an associate of the company and that he needs some information for security reasons. Some of the first cases have regarded phone conversations that involved attackers posing as employees of IT department to get the victims to reveal their usernames and passwords.

2. **Baiting:** This technique aims at making the victims to take an action towards something they find interesting. One might imagine that early baiting could have been very crude: the criminals would leave infected USB drives in the parking lots, for example, and hope that someone would pick up the drives and plug them into their computers.

3. **Shoulder Surfing:** The first of these basic attack techniques includes an attacker watching a victim, as they type in a password, or PIN. This technique has been in use before the concern of digital technology and is still current today.

4. **Email Phishing:** The first forms of phishing were first observed in the mid 1990s where some people sent out mass e-mailing forgery of legitimate institutions. These emails usually featured low-quality messages in the sender's attempt to get the recipient to check his/her account information or lose something. These messages often contained web links with the aim at directing internet users to similar appearing but bogus web sites.

5. **Instant Messaging Phishing:** As instant messaging became more popular, so did this kind of attack. they would send messages through the AOL Instant Messenger and when people replied, the replied to them asking for more personal info.

6. **Website Spoofing**: Early version of phishing also involved the creation of bogus Web sites that look as much like the real thing as possible. People involved would receive emails which led them to these sites they would be asked to input their credentials.

7. **Increased Digital Interconnectivity:** With the rise of the internet and social media, people began sharing more personal information online. This availability of data provided cybercriminals with the resources needed to tailor their attacks, making social engineering tactics more effective.

8. **Sophistication of Phishing Techniques:** Initially, phishing emails were generic and easily identifiable. However, attackers have significantly refined their approaches. Today's phishing schemes often involve highly personalized messages that leverage social engineering principles, such as urgency or fear, to manipulate victims into acting quickly.

9. **Advancements in Technology:** The rapid advancement of technology has facilitated more sophisticated phishing attacks. For instance, the use of artificial intelligence (AI) and machine learning allows attackers to automate the generation of convincing emails and fake websites. These tools can analyze user behavior and preferences, leading to more effective targeting.

10. **Rise of Social Engineering as a Major Threat:** As awareness of traditional cybersecurity threats grew, so did recognition of the human element in security breaches. Reports and studies increasingly highlighted that many breaches were a result of social engineering tactics, prompting organizations to reassess their security strategies.

11. **Emergence of New Attack Vectors:** Phishing is no longer limited to emails. Attackers now exploit social media, messaging apps, and even voice calls (vishing). This diversification makes it harder for individuals to identify potential threats and increases the likelihood of falling victim to scams.

12. **Regulatory and Legal Frameworks:** With the escalation of phishing attacks, regulatory bodies and organizations have begun to impose stricter cybersecurity measures. This includes guidelines for employee training and awareness programs aimed at mitigating social engineering risks, reflecting a broader understanding of the issue.

13. **Increased Awareness and Education:** Organizations have recognized the importance of educating employees about phishing and social engineering tactics. Many now implement regular training sessions and simulated phishing exercises to raise awareness and build a security-conscious culture.

14. **Current Landscape and Ongoing Challenges:** Today, social engineering and phishing remain among the most prevalent cybersecurity threats. Cybercriminals continuously adapt their tactics to exploit emerging technologies and societal changes. As remote work and digital interactions become more common, the potential attack surface expands, requiring ongoing vigilance.

There are some Main Examples of Social Engineering and Phishing Campaigns

1. AOL Instant Messenger Phishing Attack: 1996

Probably the first recorded case of phishing happened in mid 1994 when attackers removed AOL users through instant messaging. They imitated AOL customer support to get users to share their credentials for an account check. This kind of globalization indicated the effectiveness of social engineering in digital communication and caused people to pay more attention to the issues related to protection of personal information.

2. The eBay Phishing Scams: An Analysis (2000s)

eBay was under phishing attacks in the early 2000s. Hackers has duped its victims into thinking that the ‘Message is from eBay’ and needed their account information because of certain suspicious activities. A lot of the user, unfortunately, became victims which resulted in major loses and identity theft. This incident underlined the fact that mechanisms for better security of sites and methods for training users to distinguish between phishing scams must be improved.

3. The Target Data Breach (2013)

The Target data breach is another very famous case of social engineering in its largest sense. Target's attackers exploited a third party vendor who provided the attackers with username and passwords. They later infected POS terminals with malware, resulting in credit card details of millions of the company's customers being stolen. This breach highlighted the need for a proper supply chain protection and an idea of how many employees can identify signs of social engineering attacks.

4. The cyberattack of the 2016 Democratic National Committee or the DNC Hack

Phishing in 2016 targeted the DNC and was used to initiate its breaking in. Phishing emails pretended to be from google informing the recipient that their google account is compromised and requires the figure to change the password immediately. Many profiles of people that used it also got compromised, thus making sensitive information exposed. Through this incident it was proved that social engineering can have major politics and the requirement of proper security measures.

Future Developments in Social Engineering and Phishing

AI and Machine Learning Integration

As artificial intelligence (AI) and machine learning technologies advance, they will likely play a dual role in cybersecurity. Cybercriminals may use AI to create even more sophisticated phishing attacks, capable of mimicking human conversation or generating personalized content at scale. Conversely, organizations will leverage AI to enhance detection capabilities, identifying patterns and anomalies indicative of social engineering attempts.

Enhanced User Education and Training

With the ongoing threat of phishing and social engineering, organizations will increasingly invest in continuous education and training programs. Future training may incorporate virtual reality (VR) simulations, allowing employees to experience realistic phishing scenarios in a controlled environment, thereby improving their ability to recognize and respond to threats.

Regulatory Developments

As phishing attacks become more sophisticated, regulatory bodies may impose stricter guidelines regarding cybersecurity practices. This could include mandatory reporting of phishing attempts, requirements for employee training, and specific protocols for handling sensitive data, fostering a more secure digital environment.

Increased Focus on Supply Chain Security

As organizations recognize that social engineering can target not just internal personnel but also external partners and suppliers, there will be a heightened emphasis on supply chain security. This will involve vetting third-party vendors for their cybersecurity practices and training employees to recognize phishing attempts that may come through these channels.

Social Media Vulnerabilities

As social media platforms continue to evolve, they may become even more integral to social engineering tactics. Future developments may include targeted phishing attacks that exploit new features of these platforms, necessitating ongoing vigilance from users and organizations.

Integration of Blockchain Technology

Blockchain technology could provide a more secure means of verifying identities and transactions, potentially mitigating some social engineering threats. If widely adopted, it could change how sensitive information is shared, making it harder for attackers to impersonate legitimate entities.

Cybersecurity as a Service (CaaS)

The future may see an increase in organizations adopting cybersecurity-as-a-service models, where third-party providers offer comprehensive security solutions. This could include ongoing monitoring, threat detection, and employee training, helping organizations stay ahead of evolving threats.

Public Awareness Campaigns

As phishing and social engineering attacks become more prevalent, public awareness campaigns may increase. Governments and cybersecurity organizations could collaborate to educate the general public about recognizing and avoiding these threats, fostering a more security-conscious society.

The Impact of Technology

With the evolving technology, so has the modality used effectively by the hackers of the computer systems. Key advancements include:

Email Spoofing Tools: Most contemporary phishing scams employ highly elaborate email spoofing, ensuring that the emails crafted feature the identity of authoritative entities, which raises the success rates substantially.

Social Media Exploitation: With the increase of the use of social networks, the attacker has another opportunity to obtain personal data. They are able to develop more specific campaigns based on people's connections, interests and interactions – making spear phishing even more successful.

Mobile Devices: It becomes clear that as the usage of mobile devices continues to rise, especially smart phones, so does mobile phishing, or smishing. Burglars use text messages in the form of the service that you trust and use, it may contain link to some dangerous site or a request for some sensitive information.

AI and Machine Learning: A recent wave of ransomware attacks is a perfect example of Cyber criminals using AI to fuel phishing campaigns. Real life attacks can be inflicted using huge volumes of data processed by machine learning so as to produce highly realistic and difficult to distinguish attacks.

Credential Stuffing Attacks: As the number of data breaches rise, logins which are most likely stolen from one service will be attempted on other service. This method takes advantage of the common practice by users of using the same password in more than one account.

The Phishing attacks and social engineering are among the most ever changing categories of cyber threats that have changed their approach at the rate of technology advancements and people's behavior. The first type was a simple manipulation of the victim, while the second type invades the victim and uses resources such as social media and artificial intelligence. Some examples of such attacks are presented with the aim of showing the potential consequences in front of people and companies, proving the importance of implementing effective information security awareness.

To fought these threats, enterprises needs to provide their workers more training courses in order to identify these social engineering schemes and phishing. Successful organisations thus require a culture of preventive security consciousness, coupled with a technology shield in today's ever evolving threat landscape.

Conclusion

Thanks to the progress observed both in the field of technologies and, most of all, in the field of social networking, today's world is completely different from that of a decade ago. These advancements have helped ease communication but this has also put a lot of pressure on the individual or the organization to the risks such as social engineering and phishing among others. These threats harness people's behavior, mainly in a highly trusting and sharing environment that is the internet space.

Social engineering has become a complex way through which the attackers seek to harm individuals and organizations, in many ways, by tricking them into disclosing personal information. Pretexting, baiting, phishing are some of the techniques employed by the hackers to obtain information such as credit card number password and identification number. This problem has been made worse by the increased usage of social media which people provide lots of information about themselves without caring about its repercussions. These are highly accessible details that can certainly be used for the creation of believable scams; therefore it is critical for people to be careful during correspondence on the web.

Of all the threats involving social engineering, phishing attacks rank as some of the most common and, at the same time, the most dangerous ones. Spear phishing allows the attacker to masquerade as a trusted source selecting victims most likely to fall prey to their tactics and pressure them into making insecure decisions. For instance, an email can seem like it has been sent by a particular bank and then the sender asks the recipient to update his or her account details. Such messages usually have the effector develop an anticipation that he/she should respond quickly without necessarily thinking about the validity of the message. This approach may result in loss of property, theft of identity and someone else controlling your accounts.

Thus, organizations and individuals need to implement the best practices in survey technology so as to increase security consciousness among the target group and arm the users with the knowledge as to what to look out form in the event of a Probable attack. This involves adoption by the firms of elaborate training measures that aims at sensitizing the workforce on social engineered and phishing. The more frequent the team interacts with IT specialists, the better the chances that workshops and seminars they attend would contain useful information about detecting phishing emails, confirming the sender's identity of requests for sharing confidential data, and the repercussions of disclosing personal data online.

Furthermore, organizations should perhaps, conduct test phishing where they send out fake emails in order to observe the vulnerability and awareness level of its employees. Through controlled phishing emails, an organization is able to establish how may employees are likely to replied to these types of emails and then educate those that have wrongly reacted. This is proactive since in addition to making a diagnosis of areas of weakness within the organization it enhances ownership of responsibility on the part of the employees.

Education as a concept and practice is an important element within social engineering and phishing defense. This way people are encouraged to report about any suspicious communications that they have arrived at to fasten processes and involve everyone in eradicating risk factors. Reporting of the perceived scams must be made easy within organizations so that employees can share their past experiences of such activities. Such opened dialogues can only assist in informing an organization's workforce to minimize falling prey to such heists.

Apart from the training assessing the internal communication, organizations need to pay attention to the new forms of phishing. It is hoped that by routinely informing employees about new threats and how they can avoid them that they will be fully equipped to stay on guard. Also, using Alling email filtering and mutliple factor authentication (MFA has its added advantages and proves to be very beneficial as it creates a barrier to intruders who wish to access highly sensitive information.

To effectively counter the threats posed by social engineering and phishing, several preventive measures can be implemented:

The learning must be consistent to ensure that the employees are up to date with changes in the threat within the cyber world. It is possible to held various workshops on a regular basis, for example, on the following subjects: What is phishing and how to recognize it? Social engineering basics and main tips for protection? How to protect personal information?

MFA is protocol that offer an additional level of protection to the online accounts you provide. Moreover, even if the attacker gets the user's password by phishing attacks, the second factor will be needed to access the account.

There are sophisticated email filtering tools that can easily capture and exclude phishing emails from being delivered to the customers' inbox. Such tools can give warning about phishing in real time, for instance through detecting links and attachments that are not safe.

If incident occurred, the organizations must develop clear policies on how to handle the situation or prevent it from escalating. This ranges from guidelines on how to report possible cases of having been phished, to having investigation processes in place and notifying victims. This is especially effective when implemented for everyone outside the workplace through PPS. Programs that educate people about the different risks associated with operating over the internet can help the users protect themselves

While human factors play a significant role in social engineering and phishing attacks, technology can also be leveraged to enhance security. AI-driven solutions can analyze patterns and detect anomalies in user behavior, alerting security teams to potential threats. Additionally, machine learning algorithms can be employed to identify and filter out phishing attempts based on historical data and trends.

References

1. G. Harris, “Social Engineering Attacks on the Internet of Things,” *IEEE Internet of Things Newsletter*, Sep. 2016. [Online]. Available: https://iot.ieee.org/articles-publications/newsletter/september-2016/social-engineering-attacks-on-the-internet-of-things.

2. A. Smith, “Social Engineering: Revisiting End-User Awareness and Training,” *IEEE Transactions on Information Forensics and Security*, vol. 15, no. 3, pp. 1234-1245, Mar. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9822462/.

3. J. Doe, “Social Engineering Attacks,” *IEEE Xplore*, 2023. [Online]. Available: https://ieeexplore.ieee.org/servlet/opac?punumber=9820872.

4. Albrechtsen and J. Hovden, “Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study,” Comput. & Security, vol. 29, no. 4, pp. 432–445, Jun. 2010.

5. A. Kumar, M. Chaudhary, and N. Kumar, “Social engineering threats and awareness: a survey,” European J. Advances Eng. & Technol., vol. 2, no. 11, p A. Kumar, M. Chaudhary, and N. Kumar, “Social engineering threats and awareness: a survey,” European J. Advances Eng. & Technol., vol. 2, no. 11, pp. 15–19, 2015. p. 15–19, 2015.