International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 434-444 www.ijaem.net ISSN: 2395-5252

Hacking Techniques and Future Trend: Social Engineering (Phishing) and Network Attacks (DOS/DDOS)

Teoh Chun Hwung[1], Mohamad Fadli Zolkipli[2]
1 Awang Had Salleh Graduate School, School of Computing, Universiti Utara Malaysia, Kedah, Malaysia
2 School of Computing,Universiti Utara Malaysia,Kedah, Malaysia..

Date of Submission: 10-07-2023 Date of Acceptance: 20-07-2023

ABSTRACT: The world of social engineering, specifically phishing, and network attacks, with a focus on understanding the hacking techniques employed and exploring the future trends in these domains. It examines the significance of social engineering in exploiting human psychology and manipulating individuals to divulge sensitive information, emphasizing the growing threat of phishing attacks. Additionally, investigates community attacks including denial-of-provider (DoS) and allotted denial-of-carrier (DDoS) assaults, losing light on their disruptive nature and the potential effects for organizations. Mitigation strategies and countermeasures to protect against these attacks are discussed, highlighting the importance of proactive defence mechanisms and robust security measures. Besides that, explores the rising traits in healthcare Internet of Things (IoT) networks, analyzing the vulnerabilities and protection challenges they present, especially within the context of the COVID-19 pandemic.Furthermore, emphasizing the need for continuous research, collaboration, and the implementation of effective security measures to safeguard against social engineering and network attacks, ultimately ensuring a secure digital environment for individuals and organizations alike.

KEYWORDS:social engineering, hacking techniques, network attacks, vulnerabilities, Mitigation strategies, countermeasures, emerging trends, Internet of Things

I. INTRODUCTION

In today's interconnected world, the rapid advancement of technology has brought about numerous opportunities, but it has also given rise to significant security risks and threats. The statistics provided by Cybersecurity Malaysia's MyCert indicate a concerning increase in reported incidents across various categories of cyber threats[1].

Examining the most recent data available for the year 2023 (from January to May), we observe that the total reported incidents stand at 2,363, indicating a potential continuation of the trend. Notably, categories like fraud (1,509 cases) and malicious codes (259 cases) are prominently featured, underscoring the persistent nature of these threats[1].

#	JAN	FEB	MAC	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Fraud	235	222	340	338	374	0	0	0	0	0	0	0	1,509
Vulnerabilities Report	10	9	9	2	3	0	0	0	0	0	0	0	33
Intrusion	72	39	46	30	39	0	0	0	0	0	0	0	226
Spam	13	6	5	4	6	0	0	0	0	0	0	0	34
Intrusion Attempt	22	17	17	15	26	0	0	0	0	0	0	0	97
Denial of Service	0	1	2	4	0	0	0	0	0	0	0	0	7
Content Related	12	37	53	45	51	0	0	0	0	0	0	0	198
Malicious Codes	24	45	71	62	57	0	0	0	0	0	0	0	259
	388	376	543	500	556	0	0	0	0	0	0	0	2,363

Figure 1: General Incident Classification Statistics 2023 (Jan-May)[1]

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 434-444 www.ijaem.net ISSN: 2395-5252

These statistics highlight the pressing need to understand and address the hacking techniques that cybercriminals employ to exploit vulnerabilities in both technological infrastructure and human behaviour.

Cybercriminals have become increasingly sophisticated, utilizing the internet to carry out cyber-attacks, often targeting technological infrastructure and exploiting human weaknesses[2]. The dissemination of big data and the pursuit of competitive advantages have further incentivized these activities [3]. Importantly, the weak link often lies with users themselves, making them susceptible targets for exploitation [4].

The sizeable adoption of statistics and communique technology has extended the risk panorama, particularly thru avenues which include social engineering attack (SE) and denial-of-carrier (DoS) attack[5][6]. DoS attacks aim to render network resources and systems unavailable, disrupting connectivity and impeding access for legitimate users [7]. These attacks can exhaust critical resources and bring entire systems to a halt [8].

Understanding the mechanisms and implications of hacking techniques such as social engineering (phishing) and network attacks (DoS/DDoS) is crucial for individuals and organizations to effectively protect themselves in an evolving cybersecurity landscape. By examining these techniques and their future trends, this research paper aims to provide valuable insights and recommend mitigation strategies to combat these threats effectively.

In conclusion, as cyber threats continue to proliferate, it is imperative to comprehend the hacking techniques used by malicious actors and remain vigilant against evolving trends. By exploring the various aspects of social engineering and network attacks, this research paper seeks to contribute to the understanding of cybersecurity challenges and foster a proactive approach to protecting digital assets and personal information.

II. LITERATURE REVIEW

A. BACKGROUND

The field of cybersecurity has undergone significant transformations in recent decades, driven by the evolving motivations and tactics of hackers. Initially pushed via curiosity or a preference to showcase technical abilities, hackers have increasingly more shifted toward malicious activities including facts theft, denial-of-services (DoS) attacks, and malware deployment.

In Malaysia, one of the foremost challenges faced by cybersecurity professionals relates to the proliferation of social engineering, phishing, and network attacks. These strategies exploit human vulnerabilities and manage pc structures to advantage unauthorized get right of entry to sensitive data and sources.

Analyzing General Incident Classification Statistics for the years 2021 and 2022 reveals the magnitude of the problem. In 2021, a total of 10,016 incidents were reported, with categories such as fraud (7,098 cases) and malicious codes (648 cases) being particularly prevalent. While there was a decrease in reported incidents in 2022, with a total of 7,292 cases, threats such as fraud (4,741 cases) and malicious codes (1,023 cases) remained significant concerns [1].

B. SOCIAL ENGINEERING AND PHISHING

Social engineering encompasses a number strategies hired to misinform people into revealing private statistics or acting harmful moves. Phishing, a specific sort of social engineering attack, entails the use of fraudulent emails or text messages impersonating legitimate resources like banks or credit score card organizations. These deceptive communications often prompt victims to click on malicious links or attachments, leading to malware installation or redirection to fake websites for the purpose of stealing personal information [9].

DoS attacks aim to render computer systems or network resources inaccessible to legitimate users. Attackers achieve this by overwhelming targets with excessive traffic or exploiting software vulnerabilities. Distributed denial-of-service (DDoS) attacks, on the other hand, employ multiple computers, typically controlled by a single attacker through a botnet, to launch the attack [10].

C. IMPLICATIONS AND CASE STUDIES

Social engineering, phishing, and network attacks have had severe repercussions in Malaysia, including substantial financial losses, theft of personal data, and disruptions to critical infrastructure. A notable social engineering incident is the 2020 Maybank data breach, where hackers gained unauthorized access to Maybank's systems [11]. Millions of customers' personal facts, such as credit card numbers and Social Security numbers, were compromised. AirAsia was the subject of a DDoS assault in March 2019 that lasted for a number of hours. Customers found it challenging to make airline reservations or check in for flights as a result of the attack on AirAsia's website and mobile app [12].

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 434-444 www.ijaem.net ISSN: 2395-5252

D. Mitigation Strategies and Countermeasures

In order to address the risks presented by social engineering, phishing, and network attacks, several strategies and countermeasures have been identified. One approach is user awareness training, which involves educating individuals about the risks associated with these types of attacks. By increasing their knowledge and understanding, individuals are better equipped to recognize and avoid potential threats [13].

Another effective countermeasure is the implementation of multi-factor authentication. This approach calls for customers to provide more than one sorts of identity, such as passwords and safety codes, to gain get admission to sensitive information or systems. By adding this additional layer of security, organizations can significantly strengthen their defences against unauthorized access attempts [14].

To avoid denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, traffic filtering and rate limiting measures can be employed. Firewalls and intrusion detection systems can be used to filter out malicious traffic, reducing the likelihood of successful attacks. Additionally, implementing rate limiting controls can restrict the volume of traffic that can be directed towards specific systems or networks, further enhancing defense mechanisms against DoS and DDoS attacks[15].

Network monitoring performs a critical role in figuring out and mitigating capacity DoS and DDoS attacks. Constantly monitoring network traffic allows for the timely detection of suspicious activities, enabling organizations to take immediate action to mitigate the threats.

E. Summary of Key Findings

Social engineering, phishing, and network attacks pose an increasing threat to individuals, organizations, and society in Malaysia. These attacks can have significant financial, operational, and reputational consequences for the victims involved. However, implementing the appropriate strategies and countermeasures discussed above can assist organizations in Malaysia in mitigating the risks associated with these attacks, enhancing their overall security posture and protecting against potential damage.

III. Literature Review

A. Overview of Hacking Techniques

Hacking techniques embody an extensive range of techniques utilized by malicious actors to benefit unauthorized access to computer structures and networks.. Understanding these techniques is crucial for comprehending the evolving landscape of cybersecurity threats.

One outstanding hacking method is social engineering, which exploits human psychology to misinform and manipulate individuals into revealing sensitive information or performing certain moves. Social engineering attacks often leverage various psychological techniques to gain the trust of unsuspecting victims. Phishing is a common social engineering attack where attackers send fraudulent emails or messages that appear like from legitimate resources, tricking recipients into divulging non-public information or visiting fake websites. Pretexting involves creating a false scenario to gain the victim's trust, while a watering hole attack targets specific websites or online communities to infect them with malware. Additionally, quid pro quo attacks offer something desirable to victims in exchange for their personal information, and baiting involves leaving enticing objects or media in public places to tempt individuals into accessing malicious websites.

Another category of hacking techniques is network attacks, which exploit vulnerabilities within network systems. Denial-of-Service (DoS) attack intention to render a specific device or network unavailable via overwhelming it with immoderate site visitors, making it incapable of responding to valid requests. Distributed Denial-of-Service (DDoS) attacks, a more sophisticated variation, involve multiple computers coordinating to launch simultaneous attacks, making them even more challenging to mitigate. Furthermore, social engineering attacks are often employed in network attacks, using deceptive methods such as phishing emails to compromise network security and steal sensitive information.

Exploiting software vulnerabilities is another prevalent hacking technique. Hackers actively seek weaknesses in various software, including operating systems and web applications, to gain unauthorized access to computer systems. Buffer overflow attacks occur when an attacker overwhelms a buffer with excessive data, which can overwrite other memory locations and enable the execution of arbitrary code on the system. Cross-Site Scripting (XSS) attacks inject malicious code into web pages, exploiting vulnerabilities in web applications to steal sensitive information or compromise user sessions. Given the complexity of software and the ever-evolving nature of vulnerabilities, maintaining up-to-date software versions, applying security patches, and implementing robust firewall and security software

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 434-444 www.ijaem.net ISSN: 2395-5252

are crucial in safeguarding systems against such attacks.

Malware, including Advanced Persistent Threats (APTs), represents another significant hacking technique. Malware refers to malicious software designed to compromise computer systems or networks. APTs are a particularly sophisticated form of malware tailored to target specific organizations or individuals. Viruses replicate themselves and propagate across computer systems, causing damage such as file deletion, data corruption, and operational disruption. Worms, on the other hand, autonomously spread through networks, exploiting vulnerabilities to consume bandwidth, compromise performance, and compromise the security of connected devices. Trojans, named after the deceptive wooden horse in Greek mythology, masquerade as legitimate files or programs and, once activated, can carry out various malicious actions, including installing additional malware, creating backdoors for unauthorized access, or compromising system security and stability. Ransomware, a highly destructive form of malware, encrypts files on victims' systems, rendering them inaccessible and demanding a ransom payment for their restoration. Ransomware attacks can cause significant financial losses, operational disruptions, and compromised data security.

APTs, on the other hand, are often more sophisticated than traditional malware. They employ a range of techniques to gain access to target systems, such as spear phishing, where tailored emails are sent to specific individuals to deceive them into revealing sensitive information, watering hole attacks, which exploit trusted websites frequented by the target, and zero-day exploits, taking advantage of previously unknown vulnerabilities. APTs can remain undetected for extended periods while conducting reconnaissance, exfiltrating data, or carrying out other malicious activities.

These hacking techniques is essential for organizations and individuals to enhance their cybersecurity defenses. By staying informed about the tactics employed by hackers, implementing robust security measures, educating users about potential threats, and maintaining up-to-date software and system patches, individuals and organizations can mitigate the risks posed by these hacking techniques and ensure the security and integrity of their computer systems and networks.

B. SOCIAL ENGINEERING TECHNIQUES

Social engineering is a type of hacking that relies on human psychology to trick victims into giving up their personal information or clicking on malicious links [16].Some of the most common social engineering attack techniques are phishing, pretexting, watering hole attack, quid pro quo and baiting.

Phishing is a sort of email scam that is designed to appear to be its miles from a valid source, including a financial institution or credit card business enterprise. The email will regularly comprise a hyperlink that, whilst clicked, will take the victim to a fake internet site that looks as if the real website. Once the sufferer enters their private facts at the fake website, the attacker can thieve it.

Pretexting is a sort of social engineering attack wherein the attacker creates a fake scenario that allows you to benefit the victims believe. For example, the attacker might pose as a customer service consultant from an agency and call the victim, claiming that there is a problem with their account. The attacker will then ask the victim for non-public information, which includes their Social Security number or credit card number.

A watering hole attack is a form of social engineering attack in which the attacker objectives a specific internet site or online community. The attacker will then infect the website or network with malware. When victim go to the internet site or community, they may be infected with the malware.

A quid pro quo attack is a type of social engineering attack wherein the attacker offers the sufferer something in alternate for his or her private data. For instance, the attacker might provide the sufferer an unfastened gift or a reduction in exchange for their electronic mail address or phone number.

Baiting is a form of social engineering attack wherein the attacker leaves a bait, such as a USB pressure or a chunk of paper with a hyperlink on it, in a public area. When a person picks up the bait and clicks on the link, they'll be taken to a malicious website.

C. NETWORK ATTACK

Network attack techniques are a broad category of hacking techniques that involve exploiting vulnerabilities in network systems. These techniques can be used to disrupt network traffic, steal data, or gain unauthorized access to a network[17].

One of the most common community assault techniques is a denial-of-service (DoS) attack. A DoS attack is a try to make a computer device or network unavailable to its supposed customers. DoS attack generally contain flooding the goal with so much traffic that it's far not able to reply to valid requests.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 434-444 www.ijaem.net ISSN: 2395-5252

A more sophisticated form of DoS attack is a distributed denial-of-service (DDoS) attack. A DDoS attack involves multiple computers attacking the target simultaneously. DDoS attacks can be much more difficult to defend against than DoS attacks.

D. EXPLOITING SOFTWARE VULNERABILITIES

Software vulnerabilities are one of the most common ways that hackers gain access to computer systems. These vulnerabilities can be found in all types of software, from operating systems to web applications. Once a hacker finds a vulnerability, they can exploit it to gain unauthorized access to the system [18].

One of the most common ways that attackers exploit software vulnerabilities is through buffer overflow attacks. A buffer overflow attack occurs when too much data is written to a buffer, which can overwrite other memory locations. This can allow the attacker to execute arbitrary code on the system.

Another common way that attackers exploit software vulnerabilities is through cross-site scripting (XSS) attacks. XSS attacks occur when malicious code is injected into a web page. This code can then be executed by the victim's browser, which can allow the attacker to steal cookies or other sensitive information.

Software vulnerabilities can be very difficult to find and fix. This is because software is often complex and there are many different ways that it can be used.

E. MALWARE AND ADVANCED PERSISTENT THREATS (APTS)

Malware is a form of software that is designed to damage a pc device or community. It can be used to steal data, deploy backdoors, or disrupt operations. APTs are a sort of malware that is mainly designed to goal specific companies or individuals. They are frequently very state-of-the-art and tough to discover.[19].

Among this, viruses are a form of malicious software, commonly known as malware, that possess the ability to replicate themselves and propagate from one computer to another. Their primary purpose is to cause harm and disruption to the infected systems. Viruses can inflict damage in various ways, such as deleting important files, corrupting data, or interfering with the normal functioning of computer operations. These actions can lead to significant consequences, including loss of valuable information, system instability, and compromised security.

Another type of malware which is worms, are distinct from viruses in that they can spread autonomously through computer networks without requiring human intervention. Worms exploit vulnerabilities in network protocols or software to infiltrate and infect connected devices. Once inside a system, they can consume substantial amounts of bandwidth, congest network resources, and compromise the performance of both local and remote machines. Furthermore, worms may also engage in unauthorized data exfiltration, stealing sensitive information such as passwords or personal data, which can result in severe privacy breaches and financial losses.

Trojans, named after the deceptive wooden horse in Greek mythology, are a particularly treacherous form of malware. They disguise themselves as legitimate files or programs, often enticing users to download or execute them unknowingly. Once activated, Trojans can carry out a range of malicious actions, including installing additional malware, creating backdoors for unauthorized access, or initiating unauthorized processes that may compromise the security and stability of the infected system. Due to their ability to deceive users and remain undetected, Trojans pose significant risks to the confidentiality, integrity, and availability of data and resources.

Ransomware has gained significant notoriety in recent years as a highly destructive form of malware. This form of malicious software program encrypts files and information on a victim's pc device, rendering them inaccessible and unusable. Cybercriminals at the back of ransomware attacks then demand a ransom payment, usually in cryptocurrency, in change for supplying the decryption key or device to repair the compromised files. Ransomware attack could have devastating effects for people, corporations, and even vital infrastructure structures, causing sizeable economic losses, disruption of operations, and compromised statistics protection. The exponential rise of ransomware attacks has made cybersecurity awareness and preventive measures more crucial than ever to mitigate the risks and protect against these malicious threats.

APTs are often more sophisticated than traditional malware. They may use a variety of techniques to gain access to a target system, such as spear phishing, watering holes, or zero-day exploits. Once they have gained access, they may remain undetected for long periods of time while they gather information or carry out malicious activities.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 434-444 www.ijaem.net ISSN: 2395-5252

IV. FUTURE HACKING TREND

A. ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML) IN HACKING

Artificial Intelligence (AI) and Machine Learning (ML) have emerged as significant technological advancements with potential implications for hacking techniques and future trends. The recent developments in AI have sparked discussions on the consequences of deploying AI systems in various domains, including the realm of hacking.

The workers' perspectives on AI systems in the context of hacking reflect a realistic understanding of the technology. The AI systems as powerful tools rather than collaborators or partners. They acknowledge the potential benefits of AI in augmenting human capabilities, such as assisting with decision-making processes and analyzing large amounts of information efficiently. However, AI systems as having the ability to truly cooperate or collaborate with humans on a human-to-human level, which echoes the limitations of earlier human-machine cooperation models. As AI continues to evolve, it is essential to consider the implications of AI and ML in the field of hacking. The primarily focused on workers' perspectives in France and specific domains, it sheds light on the realistic view of AI systems as tools and the need for understanding their outputs, explainability, and trustworthiness [20] .These factors play a crucial role in determining the adoption and utilization of AI systems in hacking practices.

In workers' viewpoints and experiences regarding AI systems in hacking is vital for anticipating future hacking trends and developing effective countermeasures. By considering the potential benefits and limitations of AI and ML in hacking, policymakers, researchers, and cybersecurity professionals can develop comprehensive strategies to mitigate the emerging risks associated with the use of AI-powered hacking techniques.

B. INTERNET OF THINGS (IOT) EXPLOITATION

In the realm of cybersecurity, a prominent trend on the horizon is the exploitation of Internet of Things (IoT) devices. The IoT, a burgeoning network of interconnected physical objects linked to the internet, holds vast potential for transforming various industries. However, alongside its benefits, the IoT also introduces new security vulnerabilities.

Among these vulnerabilities is the ease with which IoT devices can be compromised. Oftentimes, these devices suffer from inadequate security measures, rendering them susceptible to hacking. Once an attacker gains access to an IoT device, a wide array of malicious activities can be carried out. These include launching Distributed Denial-of-Service (DDoS) attacks, where the attacker overwhelms a target server with excessive traffic, rendering it inaccessible to legitimate users. Additionally, attackers can pilfer sensitive data, ranging from personal information to financial records, stored within IoT devices. Moreover, they can commandeer compromised devices to assemble botnets—networks of infected computers under the attacker's control.

Exploiting IoT devices is poised to become a prevalent hacking trend in the future, driven by several factors. Firstly, the number of IoT devices is projected to skyrocket in the coming years, providing hackers with an expanded pool of potential targets. Secondly, the growing complexity of IoT networks poses a significant challenge to securing them effectively, leaving vulnerabilities ripe for exploitation. Lastly, the increased integration of IoT devices in critical infrastructure, such as power grids and transportation systems, amplifies the risk of impactful and far-reaching attacks [21].

C. MOBILE DEVICE EXPLOITATION

Mobile devices have become an integral part of our daily lives, providing us with instant connectivity and access to a wealth of information. As technology continues to evolve, so do the methods employed by hackers to exploit vulnerabilities in mobile devices. Understanding and preparing for future hacking trends in mobile device exploitation is crucial in ensuring the security of our personal and sensitive information [22].

The widespread use of smartphones and tablets, hackers are increasingly focusing on developing sophisticated malware specifically designed for mobile platforms. These malicious programs can compromise a device's security, steal sensitive data, or even gain unauthorized access to personal information. As mobile operating systems become more complex, hackers are finding new ways to exploit vulnerabilities, making it essential for mobile users to remain vigilant and employ robust security measures.

Social engineering attacks have been a prevalent hacking technique, and they are expected to grow in the realm of mobile device exploitation. Hackers often employ psychological manipulation to deceive users into divulging sensitive information or installing malicious applications. This trend is likely to continue as hackers leverage the increasing reliance on mobile devices for various online activities. It is crucial for users to be cautious when

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 434-444 www.ijaem.net ISSN: 2395-5252

interacting with unsolicited messages, links, or requests for personal information, even on trusted platforms.

The rise of mobile banking and digital payment systems, hackers are shifting their focus towards exploiting vulnerabilities in these platforms. Mobile devices often store financial data and payment credentials, making them lucrative targets for cybercriminals. The future trend of mobile device exploitation will likely involve sophisticated attacks aimed at intercepting sensitive financial information, compromising transaction security, or gaining unauthorized access to banking applications. Users must adopt robust security practices, such as two-factor authentication and regular software updates, to mitigate these risks.

As the Internet of Things (IoT) continues to expand, mobile devices are increasingly becoming the central control hubs for various connected devices. This integration creates new avenues for hackers to exploit vulnerabilities in mobile devices and gain unauthorized access to IoT networks. Future hacking trends in mobile device exploitation may involve attacks that compromise IoT devices, leading to privacy breaches or even the manipulation of critical infrastructure. Ensuring the security of mobile devices and implementing strong encryption protocols will be vital to protect against such threats.

D. Social Engineering and Psychological Manipulation

Social engineering and psychological manipulation techniques have long been employed by hackers to exploit human vulnerabilities in order to gain unauthorized access to sensitive information. As technology advances, these techniques are expected to evolve and become even more sophisticated. Understanding the future trends in social engineering and psychological manipulation is crucial in combating cyber threats and protecting individuals and organizations from malicious attacks [23].

In the future, hackers are likely to leverage advanced personalization techniques to carry out highly targeted spear phishing attacks. By gathering publicly available information from social media platforms and other sources, attackers can create tailored messages that appear genuine and trustworthy. These personalized phishing attempts increase the likelihood of individuals falling victim to such attacks, as the messages are designed to exploit their specific interests, affiliations, or relationships. Individuals and organizations must remain cautious and employ robust email filtering and security awareness training to mitigate the risks associated with these evolving social engineering tactics.

The rise of deepfake technology and artificial intelligence (AI), hackers may exploit these tools to deceive individuals and manipulate their behaviour. Deepfakes are synthetic media, such as videos or audio recordings, that are convincingly altered to depict false information or events. In the future, hackers might use deepfakes to impersonate trusted individuals, such as company executives or friends, and manipulate targets into divulging sensitive information or performing malicious actions. Combating these threats will require advanced detection algorithms, increased media literacy, and critical thinking skills to identify and verify authentic communication.

As social media platforms continue to play a significant role in our lives, hackers are likely to exploit psychological vulnerabilities associated with online interactions. Social media platforms provide a wealth of personal information that can be leveraged to manipulate individuals and influence their actions. Future hacking trends may involve the use of persuasive messaging, emotional manipulation, or fake news to exploit individuals' trust and compromise their security. Users should be cautious about the information they share online, exercise critical thinking, and employ privacy settings to minimize the potential impact of such psychological exploitation.

The risk of insider threats and human manipulation within organizations is expected to grow in the future. Hackers may employ social engineering techniques to exploit employees' trust, coerce them into sharing sensitive information, or gain unauthorized access to corporate systems. This can result in significant financial and reputational damage. Organizations must implement robust security protocols, conduct regular employee training, and enforce strict access controls to mitigate the risks associated with insider threats and human manipulation.

V. Discussion

A. Significance of Social Engineering (Phishing) and Network Attacks

Phishing attacks have emerged as a significant and growing threat for organizations, where deceptive messages are used to manipulate individuals into revealing sensitive information or engaging in fraudulent activities. While IT departments play a vital position in implementing institutional responses to mitigate these attacks, the choices and moves of person employees also play a essential function in an business enterprise's susceptibility to phishing attempt. Understanding

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 434-444 www.ijaem.net ISSN: 2395-5252

the significance of social engineering (phishing) and network attacks is essential for organizations to develop effective strategies in combating these threats.

Some employees possess a deep understanding of phishing techniques and associated risks, while others have limited knowledge in this area. This variation in awareness and competency highlights the importance of providing comprehensive education and training to enhance employees' ability to identify and respond appropriately to phishing attempts [24].

To empower employees as collaborators in an organization's anti-phishing efforts, it is crucial for organizations to embrace a range of educational initiatives. This includes providing non-expert users with more extensive education on organizational processes and the consequences of falling victim to phishing attacks. By enhancing employees' understanding of the potential impact of phishing, organizations can foster a culture of vigilance and encourage proactive measures to counteract these threats.

B. Mitigation Strategies for Social Engineering and Network Attacks

Social engineering and network attacks pose significant threats to individuals and organizations, necessitating effective mitigation strategies. This section discusses various strategies to mitigate the risks associated with these attacks and protect against potential vulnerabilities [25].

One of the fundamental strategies in combating social engineering attacks is to provide comprehensive education and training to employees. By raising awareness about common attack techniques, such as phishing, pretexting, and baiting, employees can recognize and avoid potential threats. Training should cover topics such as identifying suspicious emails, verifying the legitimacy of requests for sensitive information, and maintaining strong password hygiene. Regular training sessions and simulated phishing exercises can reinforce security practices and help employees stay vigilant.

Furthermore, performing regular security audits and assessments helps identify vulnerabilities in systems, networks, and applications that could be exploited by attackers. Vulnerability scans, penetration testing, and code reviews should be conducted to identify weaknesses and promptly address them. Additionally, staying up to date with security patches and software updates is crucial to mitigate known vulnerabilities that attackers might exploit.

C. Emerging Trend and Future Challenges

The field of hacking techniques, social engineering (phishing), and network attacks (DOS/DDOS) is constantly evolving, presenting emerging trends and future challenges. This section discusses some of these trends and challenges, highlighting the need for proactive measures and advancements in security practices.

The increasing use of healthcare Internet of Things (IoT) networks, there is a growing concern regarding their security and the protection of sensitive patient data. The COVID-19 pandemic has further emphasized the importance of leveraging healthcare IoT technologies for remote monitoring and care. However, these networks are susceptible to cyberattacks due to vulnerabilities in communication protocols, authentication mechanisms, and medical devices. Future trends in securing healthcare IoT networks involve the adoption of end-to-end encryption, robust authentication and authorization mechanisms, and the development of specialized security protocols. Research efforts should focus on enhancing security frameworks, exploring machine learning algorithms for threat detection, and reducing the network architecture and maintenance costs while ensuring optimal security outcomes [26].

Furthermore, social engineering techniques, such as phishing, continue to be a significant threat in the hacking landscape. Attackers exploit human vulnerabilities to deceive individuals and gain unauthorized access to sensitive information. The emerging trend in social engineering attacks involves sophisticated approaches, including personalized and targeted phishing campaigns. To counter these threats, organizations must continually educate and train employees to recognize and respond effectively to social engineering attempts. Ongoing security awareness campaigns, simulated phishing exercises, and regular communication channels with IT professionals are crucial mitigation strategies. Future challenges lie in adapting to evolving social engineering techniques and devising innovative methods to detect and prevent such attacks [27].

As hacking techniques and network attacks continue to evolve, the field of cybersecurity must advance to stay ahead of cybercriminals. This involves continuous research and development of advanced threat detection and prevention mechanisms, leveraging artificial intelligence and machine learning algorithms. Emerging technologies such as blockchain and secure multiparty computation hold promise for enhancing the security of sensitive data and preventing

unauthorized access. Additionally, collaborations between academia, industry, and government agencies are vital to share knowledge, exchange best practices, and develop robust defence strategies against emerging hacking trends.

VI. CONCLUSION

The world of hacking techniques and future trends, with a specific focus on social engineering (phishing) and network attacks (DOS/DDOS). These had delved into the intricacies of these malicious practices, their impact on individuals and organizations, and the evolving landscape of cybersecurity. Throughout the analysis, several key insights and findings have emerged.

Firstly, social engineering techniques, particularly phishing, have become increasingly sophisticated, posing a significant threat to individuals and organizations alike. Attackers exploit human vulnerabilities to deceive users and gain access to sensitive information. As a result, it is crucial for organizations to invest in robust security measures, including comprehensive security awareness programs, employee training, and regular communication channels with IT professionals. By empowering employees and enhancing their understanding of social engineering tactics, organizations can fortify their defences and mitigate the risks associated with these attacks.

Secondly, network attacks, such as denial-of-service (DoS) and distributed denial-of-service (DDoS), continue to plague the digital landscape. These attacks disrupt the availability of services, causing significant financial losses and reputational damage. To counteract these threats, organizations must adopt proactive measures, such as implementing robust network security infrastructure, employing traffic monitoring and anomaly detection systems, and leveraging scalable cloud-based resources to mitigate the impact of such attacks. Collaborative efforts between organizations, internet service providers, and cybersecurity experts are also crucial in developing effective defence strategies.

Furthermore, emerging trends and challenges have highlighted the significance of securing healthcare Internet of Things (IoT) networks and improving predictive models in software engineering. Healthcare IoT networks play a vital role in remote patient monitoring and care. However, these networks are vulnerable to cyberattacks, necessitating the implementation of strong security measures, including end-to-end encryption, authentication mechanisms, and specialized security protocols. Meanwhile, predictive models offer opportunities for enhancing software development processes but require attention to data quality, bias mitigation, and model accuracy.

Moreover, it is evident that the field of hacking techniques and cybersecurity is ever-evolving. To stay ahead of cybercriminals, organizations must prioritize ongoing research and development of advanced threat detection and prevention mechanisms. This involves leveraging emerging technologies, such as artificial intelligence, machine learning, blockchain, and secure multiparty computation. Collaboration among academia, industry, and government agencies is vital to share knowledge, exchange best practices, and collectively build a secure digital environment.

In the face of future challenges, the pursuit of cybersecurity excellence should remain a continuous effort. By embracing proactive measures, raising awareness, and fostering a culture of security, these can navigate the evolving landscape of hacking techniques and future trends, ensuring the safety of individuals, organizations, and society as a whole. Besides that, this can build a resilient and secure digital ecosystem that safeguards the valuable information and promotes trust in the digital realm.

VII. ACKNOWLEDGEMENT

The authors would like to thank all Schoolof Computing members who were involved in thisstudy. This study wasconducted for the purpose ofEthical Hacking & Penetration Testing ResearchProject. This work was supported by UniversitiUtara Malaysia.

VIII. REFERENCE

[1] C. Malaysia, “Cybersecurity Malaysia,” MyCert (Malaysia Computer Emergency Respond Team), 2023.

[2] M. O. B. a. A. Tepecik, “Cybersecurity,Computer Networks Phishing, Malware, Ransomware, and Social Engineering Anti-Piracy Reviews,,” 2021 - 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings, pp. 1-5, 2021.

[3] G. S. Hussain Aldawood, “Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions,” IEEE Access, vol. 8, pp. 67321-67329, 2020.

[4] N. K.-W. a. A. Wentland, ““Hacking Humans? Social Engineering and the

Construction of the „Deficient User‟ in Cybersecurity Discourses,”,” Technol. Hum. Values, vol. 46, no. 6, p. 1316–1339, 2021.

[5] H. H. M. H. E. W. Katharina Krombholz, “Advanced social engineering attacks,,” J. Inf. Secure Appl, vol. 22, pp. 113-122, 2015.

[6] S. R. H. Qwaider, “Analysis and Evaluation of Cybersecurity Techniques for Social Engineering,” Al-Azhar Univ. Fac. Eng. Inf. Technol, 2019.

[7] B. M. Nikhil Tripathi, “DoS and DDoS Attacks: Impact, Analysis and Countermeasures,” Advances in Computing, Networking and Security, 2013 TEQIP II National Conference, 2013.

[8] B. B. G. Anshuman Singh, “Distributed Denial-of-Service (DDoS) Attacks and Defense Mechanisms in Various Web-Enabled Computing Platforms: Issues, Challenges, and Future Research Directions,” International journal on Semantic Web and information systems, vol. 18, no. 1, pp. 1-43, 2022.

[9] OpenText, “What is Social Engineering,” 2019. [Online]. Available: https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering.

[10] Fortinet, “What Is the Difference Between DoS Attacks and DDoS Attacks?,” 2023. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos.

[11] A. Adegunwa, “Data Breach Involves 13 Million Users Of Maybank, Astro, and EC,” 2023. [Online]. Available: https://informationsecuritybuzz.com/data-breach-involves-users-maybank-astro-ec/.

[12] D. T. Sandle, “Security expert on AirAsia ransomware attack,” 25 November 2022. [Online]. Available: https://www.digitaljournal.com/tech-science/security-expert-on-airasia-ransomware-attack/article.

[13] J. Webster, “Security Awareness: 7 reasons why security awareness training is important in 2023,” 2023. [Online]. Available: https://www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important/.

[14] S. D. Octopus, “What is two factor authentication (2FA)?: Security wiki,” 15 August 2021. [Online]. Available: https://doubleoctopus.com/security-wiki/authentication/what-is-2fa/#security-wiki-content.

[15] K. Petrosyan, “How to Detect DDoS Attacks?,” 9 September 2022. [Online]. Available: https://securityboulevard.com/2022/09/how-to-detect-ddos-attacks/#:~:text=Web%20scanners%2C%20web%20application%20firewall,traffic%20using%20machine%20learning%20algorithms..

[16] I. G. H. M. B. Ali Derakhshan, “Detecting telephone-based social engineering attacks using scam signatures,” In Proceedings of the 2021 ACM Workshop on Security and Privacy Analytics, pp. 67-73, 2021.

[17] A. E. A. K. L. H. Atheer Alharthi, “Network Traffic Analysis for DDOS Attack Detection,” In The 4th International Conference on Future Networks and Distributed Systems (ICFNDS), pp. 1-6, November 2020.

[18] D. R. Santos, “Access Control Vulnerabilities in Network Protocol Implementations: How Attackers Exploit Them and What To Do About It.,” In Proceedings of the 28th ACM Symposium on Access Control Models and Technologies, pp. 5-6, May 2023.

[19] A. A. A. E. Meaad Alrehaili, “A hybrid deep learning approach for advanced persistent threat attack detection,” In The 5th International Conference on Future Networks & Distributed Systems, pp. 78-86, December 2021.

[20] M. Z. F. B. Tamari Gamkrelidze, “Working with Machine Learning/Artificial Intelligence systems: workers’ viewpoints and experiences,” In Proceedings of the 32nd European Conference on Cognitive Ergonomics, pp. 1-7, April 2021.

[21] J. T. J. H. G. C. S. W. X. J. P. Z. M. K. S. K. D. Linghe Kong, “Edge-Computing-Driven Internet of Things: A Survey,” ACM Computing Surveys, vol. 55, no. 8, pp. 1-41, 2022.

[22] G. S. R. T. R. G. F. D. R. V.-R. Paula Delgado-Santos, “A survey of privacy vulnerabilities of mobile device sensors,” ACM Computing Surveys (CSUR), vol. 24, no. 11s, pp. 1-30, 2022.

[23] P. L. R. F. S. W. Daniel Graziotin, “Psychometrics in behavioral software engineering: A methodological introduction with guidelines,” ACM Transactions on

Software Engineering and Methodology (TOSEM), vol. 31, no. 1, pp. 1-36, 2021.

[24] A. C. A. J. B. A. D. S. &. N.-E. C. Tally, "What Mid-Career Professionals Think, Know, and Feel About Phishing: Opportunities for University IT Departments to Better Empower Employees in Their Anti-Phishing Decisions," Proceedings of the ACM on Human-Computer Interaction, vol. 7, no. CSCW1, pp. 1-27, 2023.

[25] H. Y. W. W. W. M. D. &. L. J. Wang, "A novel cross-network embedding for anchor link prediction with social adversarial attacks," ACM Transactions on Privacy and Security, vol. 26, no. 1, pp. 1-32, 2022.

[26] J. A. M. M. J. S. R. A. N. K. A. F. H. S. Muhammad Adil, "Covid-19: Secure healthcare internet of things networks, current trends and challenges with future research directions," ACM Transactions on Sensor Networks, vol. 19, no. 3, pp. 1-25, 2023.

[27] C. V. H. B. C. J. J. J. J. N. J. J. M. L. K. S. Eric Blancaflor, "Risk assessments of social engineering attacks and set controls in an online education environment," In 2021 3rd International Conference on Modern Educational Technology, pp. 69-74, May 2021.