Sri Lanka Institute of Information Technology

BSc Honors in Information Technology

Specializing in Cyber Security

Introduction to Cyber Security - IE2022

Phishing Attacking and Social Engineering

Student ID	Student Name
IT22083678	**SAHAN H P T**

1. Abstract:

Phishing attacks and social engineering schemes are very grave cyber security fractions all over the world and they may threaten individuals as well as businesses giving offense to their dependent data. This paper deepens the aspect of malware and social engineered activities, clarifying to the reader the way attackers trick and persuade their victims to believe their lies. The report looks at the essence of three types of phishing attacks and seven social engineering techniques, and it analyzes the psychological mechanisms and the aftermath in daily life, taking the allegorical form. Evaluating scenarios from different companies and understanding the dynamics of the world today, the report demonstrates the universality of these issues and the weight of this matter for the digital world at the moment. Moreover, it points out the available preventive and response measures, concluding that user education is utmost, safeguards and incident response preparedness are also important. This report is all about broadstroking phishing and social engineering practices victims and organizations may fall prey to, and advocating for individuals and organizations alike to take the threat in hand and strive the bestone of cybersecurity resilience in a more connected digital world.

Table of Contents

2. Introduction to the topic

Concerning social engineering as well as the phishing ransom, we are faced with intellectual worries, as individual, entity or whole community can be affected by them. Today, phishing, an effective scheme perpetrated by cyber criminals that involves the sly act of misinforming individuals and tricking them into revealing sensitive information or doing something that can cause harm and destruction to their security level, is a lot more intelligent and broadly spread that it used to be.While one the other hand, social engineering relies on the exploitation of human vulnerabilities by psychological manipulation.Those can be bypassing the security measures hence gaining the access that does not have an authorization.

These days, all sorts of phishing attempts and social engineering methods epidemically colonized the Internet space because of technological advances, the ubiquity of digital communication tools, and the fact that the Web has become a global village to some extent. Fraudsters use sophisticated and often, plausible strategies such as global email scams impersonating reputable entities or AI on the phone to generate trust and achieve their malicious ends.

This report analyzes the details of phishing attacks and the frameworks of social engineering which targets unsuspecting victims, aiming to give a thorough insight of the attack methods in use. We hope that this research report will provide our readers with some insights into different cyberattacks, attack techniques and prevention strategies. Our intention is to equip people and organizations with the knowledge and tools to protect themselves and fight cybercrime in a more effective way.

3. Evolution of the topic

3.1 Historical Overview

The phishing attacks and social engineering techniques have gone through a major transformation for some time now, and they recently became even more sophisticated, something that now poses challenges not only to the individuals, but also organizations. At the start it was a series of simple attacks, email based frauds that were developed to fool people into providing their own secrecy and privacy details.Cyber-criminals have continued to improve on their phishing attacks and social engineering techniques and hence become harder to detect and stop. This has in effect led to the increase of the threats posed to individuals and organizations.With cybernetic technologies improved, spam emails and stealing of personal information were no longer restricted to the wider area, but, instead, targeted widely spread online banking and e-commerce operations. Attack's paths began ranging from social engineering like impersonation and pretexting used to manipulate human psychology and trust to deceive victims to reveal confidential information.

At the tail end of the late 2000s, activity phishing or alleged spear-phishing developed by the attacker with a target of some specific individual or organization. Conducting these hacking campaigns included as series of thorough investigations on the victims, so the attackers could carry out highly-tailored and persuasive phishing attacks with ease.It was in the nineties when advanced persistent threats (APTs) and state-sponsored attacks for going up in frequency, which mean that they began to use phishing and social engineering to target high-profile organisations like government agencies and the critical infrastructure.Nowadays, different type pfishing attacks are used as multichannel by merging channels like email, SMS and social media. The young ones are known to take advantage of the evolving technologies just as they did with previous ones i.e. deepfakes, the usage of artificial intelligence, Internet of Things (IoT) and the Metaverse.

For doing battle with these dynamic dangers a lot of importance needs to be given to the work with people and the organizations by using effective training, well-defined authentication protocols, and primary defence systems. Continuous adjustment to the protection scheme and forward faced steps against hackers of social engineering and phishing campaigns always be required to protect a continuously changing threat environment.

First-stage Phishing Assaults (the 90s) One of the earliest forms of phishing attacks that evolved is social engineering technique which purposely tricks the vulnerable users into submitting private or sensitive information to a fraudster posing to be a trusted entity [1]. At first, phishing would come by as mails, which would pretend to be from large companies/organizations, requesting you to confirm your personal or financial details.

Growth and refinement in the businesses (from the early 2000s). The term "phishing" was hatched in 1996, and the very first recorded use of the term, to my knowledge, occurred in 1997 [2].Phishing more and more widespread, with the complexity of their users has been enhanced allowing them to potential victims both in online banking and e-commerce platforms.

Social Engineering Techniques (2000s) Social engineering is tactic which tricks a victim to share sensitive information.Social engineering methods, including imitation and pretexting, became more exploited and phishing attacks indeed started employing these tools.Malefactors devised ways how to cunningly use human elements of emotions and confidence to get a victim to write their actual and secret data[3].

Targeted phishing and spear phishing (2009s). Through phishing strategies, more targeted such as spear phishing, people or organizations were taken more careful because people noticed that it was specially sent to them [4].The perpetrators invested a lot of time in learning how most email phishing attacks happen, and others developed very personalized and convincing emails that tricked users to input their credentials.

AI technology has evolved rapidly due to Advance Persistent Threats(APTs) and State-Sponsored Attacks(SOAs)(2010s).More than just malware attacks and state-sponsored espionage, cult or new religion cybercrime used phishing and social engineering techniques as their core modus operandi [5]Such advanced attacks featured a crafty approach too, which emphasized on sophisticated ones such as hacking governmental agencies and the critical infrastructure.

Multi-Vector Penetration and New Vectors – Tendencies Discovered Now and Predicted in FutureThrough malicious individuals, and crminal groups carrying out phishing attacks and using social engineering techniques ideaing integratyion of multiple vecties of email, SMS and social media have become more complex [6].To be precise, new phenomena such as the use of AI, deepfakes, and IoT were also emerging during that period.

3.2 Types of Phishing Attacking and Social Engineering

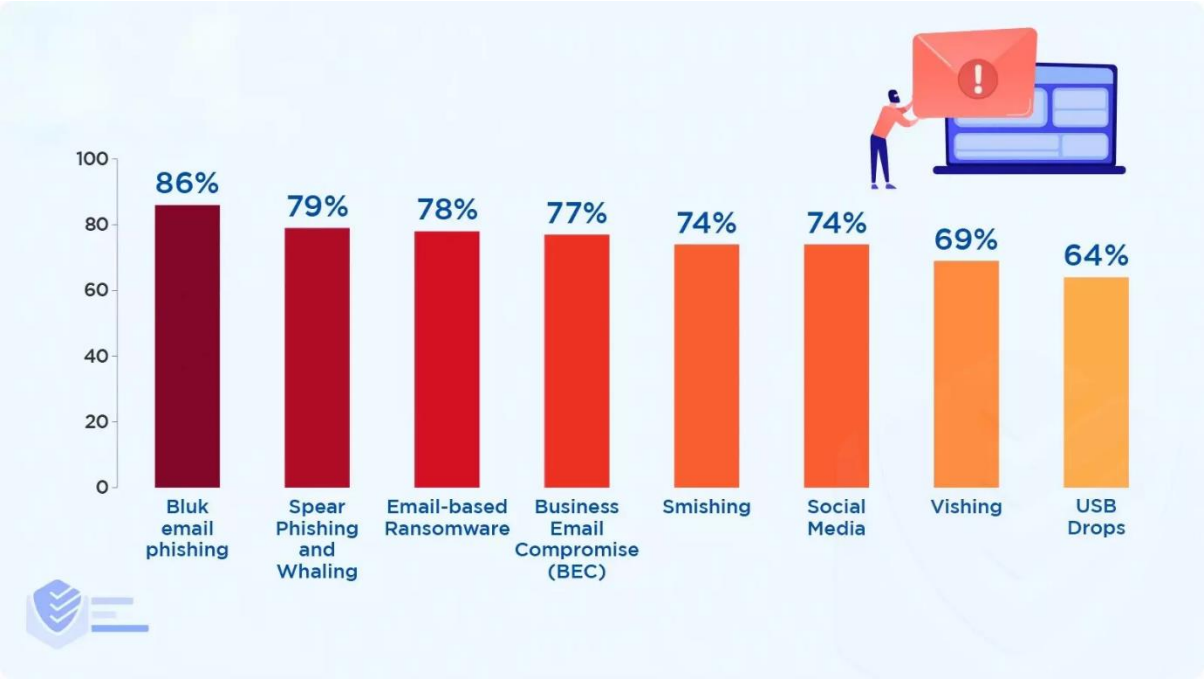

Figure 1: Types of cyber attacks on connected Phishing Attacking and Social Engineering .

Social engineering, phishing attacks, and other methods are among those cyber criminals' favourites in abusing our vulnerabilities through deceit for breakthrough to get privileged information or system. These are the malicious strategies that they use and involve portraying deceptions and manipulation of victims psychologically thus getting their important data or they give them that which compromises their security.

3.2.1 Email Phishing

Email phishing as one the most prevalent and spreading types of phishing attacks is widely used. Crminal hacker produce swindling emails which have information like bank name, online retailer shop address, or the data and service provider's publication and thus they seem to send emails from authorized sources. These mail attachments or links, they might be incorporated a malwared or as a method to steal login details or financial information from their victims. The Evolution and Continued Threat of Email Phishing Relies on Two Main Approaches: Social Engineering tactics that Create or Reinforce a Sense of Immediacy, Maintain some degree of Scare, Leverage authority, and Exploit trust in well-known brands.[6],[7]

3.2.2 Spear Phishing

A spear phishing attack, which is a phishing attack with a focus-on specific persons or organizations, is an element of a targeted phishing attack. Hackers often tend to collect exhaustive information about the target, including job positions, interests, and even secrets which they artistically apply to devise deceptive fraud emails or messages. This approach is more powerful than general fishing approach since it dives deep into the victim's private or professional life and thus make it hard to note suspension of judgment. [6],[7]

3.2.3 Smishing (SMS Phishing)

Smishing which stands for SMS phsishing is a phenomenon through which malicious individuals disguise themselves as trustworthy and via text message or SMS trick people into providing log-in credentials or visiting a dangerous website. The attackers usually pose as trustworthy entities like organizations or individuals and make the person believe what he has to protect is under attack. This is what adverse actors do to create a sense of urgency where selecting the target is portrayed as the only option and immediate action is required. The favourable environment for mass adoption of handheld devices and the driven demand for texts make phishing an interesting tendency. [6],[7]

3.2.4 Vishing (Voice Phishing)

Conning over the phone or by means of fake phone calls or voice messages is a common scam that relies on social engineering to obtain pertinent information or trick victims into transferring funds. Impersonation can occur on behalf of seemingly trustworthy entities such as banks or various government agencies, fraudulent tactics including intimidation, urgency, or authority can also be used. Victims in turn frequently surrender to such a request. [6],[7]

3.2.5 Angler Phishing

The Angler phishing is cases whereby those use social media, online discussion including chats to omit the same from the victims and therefore built trust from them. The criminals can establish a fake profile for instance and utilize the format of communications of other people to make an impression that messages are being sent from the genuine side of people. [6],[7]

3.2.6 Baiting

Baiting stands for the place where the attackers simply leave infected pendrives or CDS on any public places. Such medias as flash disks or key fob drives usually have appealing looking labels or similar to official documents in order to lure the potential victims into pointing the infected files and install the malware or give to the attackers the same access to the victim's computer. [6],[7]

3.2.7 Pretexting

In this attack, the attackers attempt to concoct an unbelievable story or a pretense that will help builds a realistic relationship with the targeted individual and then uses the rapport that they've conscientiously created to get sensitive information out of the victim. Grouping members behind various profiles such as IT support technician, law enforcement officer or even a trusted colleague can help attackers quickly build their position and authority. [6],[7]

3.2.8 Quid Pro Quo

The attacker's promise can be intentionally constructed in such a way that it can be interpreted by the victims as a service, which may include some information or soliciting access to carry out an attack on the victims. The concept of social engineering is the act of fraudulent acting on the eagerness and love of the public relating to the exchange of favor and giving of complimentary. However, the social engineering strategy can lead to the leakage of important data or unauthorized access due to the pretended reciprocity basis. [6],[7]

3.3 Vulnerabilities in Phishing Attacking and Social Engineering

3.3.1 Trust and Authority Exploitation

That is, phishers are exploiting the natural human trust in authority or someone familiar just like you. Haders use the same organizations, companies, impersonating people to release access to secret things or to perform some illegal actions [9]. Through checking the well-being of individuals/entities involved as well as the sources, this risk is controlled.

3.3.2 Emotional Manipulation

Social engineering attacks utilize emotional facets that are based on trigger points such as panic, fascination, or hunger so that victims can be directed to do as the attacker wants [10]. Educating the public on these strategies, doing away with the easy-to-notice informational stretch mark, promotes critical thinking to help minimizing these vulnerabilities.

3.3.3 Bad Email and Website verification Service

Not conducting sufficient checks of messages, websites and requests detail can end up with people not realising that they have fallen for phishing scams or disclosed crucial information by accident [11]. Implementing rigorous verification systems and getting users to be alert and attentive during verification is becoming more important every day.

3.3.4 Password and Credential Reuse

A lot of people recycle the same passwords and use them across several accounts. This strategy makes it even easier for the assailant to breach several accounts with no need to hack the accounts individually. Extending the use of a unique and strong password as well as putting in place a multi-factor authentication will assist in sorting thissecurity laps.

3.4 Impact of Phishing Attacking and Social Engineering

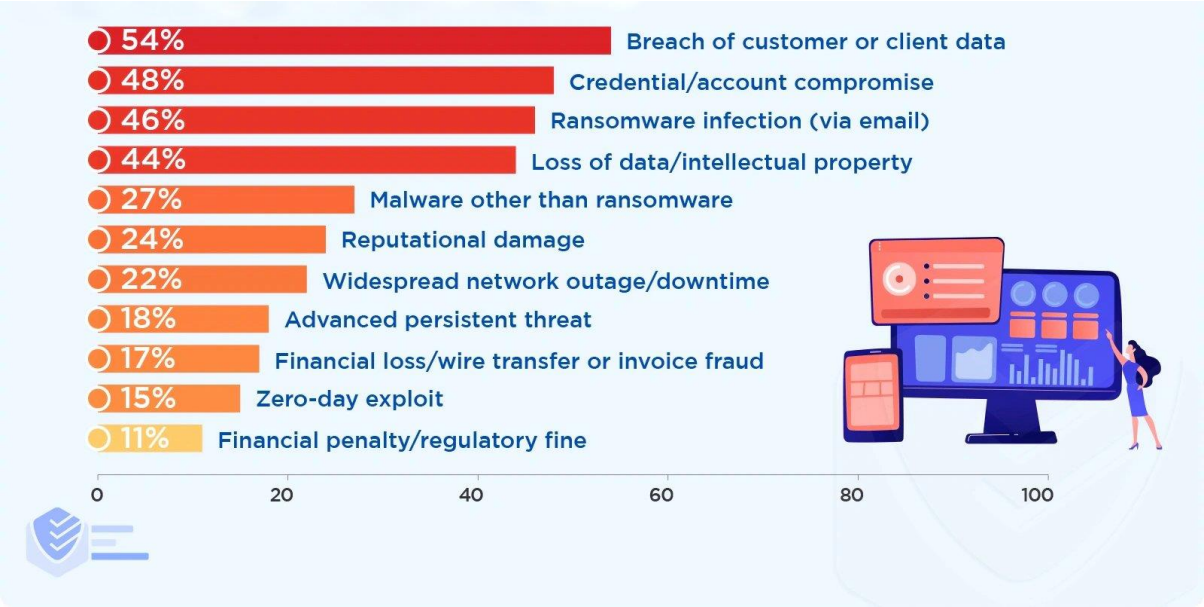

Figure 2: Impact of Phishing Attacking and Social Engineering.

3.4.1 Financial Impact

It is rather appalling to imagine the amount of money that is being lost annually in the name of phishing and social engineering schemes. Criminals can easily acquire tracing and account manipulation capabilities online. These criminals may drain accounts through fraudulent transactions, or commit identity theft taking loans and credit cards under individuals' names. Organisations experience tremendous losses from the fraud, theft of intellectual property, operational disruptions that require response and recovery actions, and fines due to non-compliance with the regulations followed by demands for legal fees following data breach. At the social level, these threats result in a severe economic damage with more than $2 billion in annual losses throughout the world and noticeable increase in the cybersecurity expense across the industries. The phishing, apparently the most dangerous one, is of great help to criminal financial ecosystems and undermines public institutions allying their trust in digital financial systems.

3.4.2 Data Breach and Privacy Violations

Data leaks by means of divulging the personal information, e.g. names, phone numbers, social security numbers and medical records, constitute a critical damage caused by phishing. For people this information susceptibility to identity theft, financial fraud, discriminatory targeting and conservative invasion of privacy wholeheartedly. Organizations sacrifice very dear corporate information to the point where the damage includes sensitive corporate data, customer records, trade secrets and intellectual property which ultimately ends up in their hands as competitors, legal problems and brand damage. Society is becoming more nervous than ever over security and privacy of data that the progression of new technologies and online services may possibly be impeded unless the problem is not taken seriously.

3.4.3 Business Disruptions and Operational Impact

While the disastrous effects of phishing attacks present themselves in multiple ways, one of the most common is when malware, like ransomware, can encrypt systems in this manner. It stops all production and sales as well as delivery of service, suppressing income. Hence, this becomes one the reasons why businesses often fail. The downtime of the remediation effort in incident response and security operations makes these productivity losses even worse. Moving past businesses, the disturbance of cyberattacks to the national critical infrastructures, namely, the power grids, communications, transportation or healthcare systems, can be dangerous to public health and safety if the threat actors bypassed the security controls and access the networks.

3.4.4 Reputational Damage

Reputational damage, although a factor that is sometimes taken for granted tends to be even more costly to organizations that becomes victims of a phishing attack. In case of personal accounts, their owners reputation can be at stake if their exploited accounts are used to spread misinformation or objectionable content. Large enterprises become the major victims of Trojans or other massive data breaches that cause consumers to lose trust in brands, causing brand image impairments manifested by marketshare contraction, client loss, devaluation and declining brand value that may take a year or even longer to recover. On a societal level, already in progress now, existing cyberattacks have started to chip at the public's belief in government institutions, large tech companies, and other strong pillars society stands on, and this could potentially be used to fuel distrust to make it hard for future technological progress to come about.

3.4.5 Emotional and Psychological Impact

Nevertheless, most often it is the financial, data, and operational damages which sting us but the emotional and psychological dangers of phishing present an equally preoccupying threat. It victims of identity theft or misuse of their personal data are often destressed and traumatised by this severe violation of their privacy. All the same, there is a chance of persistent phishing attacks and social engineering having sprinkling overplausible persuasion methodologies among society at large could bring about an environment of incessant distrust and fear on digital correspondence. Given that we heavily rely on networked interactions in personal and professional life, this dehumanizing trend can be negatively devastating on the social cohesion. Development of cybersecurity awareness and establishment of solid incident response schemes are imperative and are for protecting the cyber territory from the multifaceted pathways of phishing.

3.5 Understanding risks of Phishing Attacking and Social Engineering

Social engineering is both fundamental and quickly changing, making the deceptive acts complex. Thus, the phishers and cyber attacks require a proactive and multi-level approach the cyber security. Given the intersection growing of our personal life and professional career the traditional lines separating the personal from professional cybersecurity threats are blurred. These social media platforms, messaging apps, emails, cloud services, and collaboration tools all offer the ideal virtual soil to grow the customized phishing and social engineering campaigns that malicious actors use to launch campaigns. Remote work policies and BYOD (Bring Your Own Device) in the aftermath of COVID-19 have been marked by the fact that they keep everyone involved in making it work - from corporate to personal devices/accounts - and the clear dividing lines between the two.

However, in addition, the mind-blowing rate of progress in the field of artificial intelligence (AI) and machine learning systems brings to the scene both narrative advantages and disadvantages for this type of scheming. These new technologies are playing key roles in the security industry by expanding solutions to fight against phishing emails with a ready made detection method and malicious website/link analysis engine. Although on the one hand, AI will be utilized by attackers for massive production of precise and false phishing lures through the use of deepfakes, natural language generation, and learning for the tailored AI systems, on the other side, it will inevitably be weaponized by those who intend to attack.

An innovative type of deepfakes can be used for a phishing style attack. Nowhere will you feel safe anymore: audio messages, videos, whatever, appearing to be from your boss or a trusted coworker telling you to urgently wire the company money or share the login details. These scenarios are made possible by an AI-generated deepfake impersonation. Repentably, it can be either an email that seems genuine with details from what you are interested in, how you write, even the sound of your voice and character. This is the emerging stuff that could be an actual threat as cyber hackers can now use AI to make their social engineering more efficient than ever before.

Aside from that, the human element is indeed a prime risk factor that must be given special attention as well. Although various internet related assaults are on regular mention in media, the cyber awareness exhaustion's growth or behavior of the general public is still evident, making them more vulnerable to concur from fine looking rouses like phishing/social engineering. The malicious actors have abilities to take advantages from the vulnerabilities around mental processes and trust that are still surviving in these types of communities such as emailing and social media. The quickly multiplying phishing cases that constantly bombard individuals with emails through multiple communication channels with a strong possibility that one device will be linked to another communication device could make information security difficult for the average user to keep vigilance.

Mitigating these risks requires strong implementation of technical management along with dynamic security awareness training, advanced incident response, and the creation of a relentless cybersecurity culture with a dogged mindset. Enterprises and organizations have to be adaptive both in their cybersecurity and the failures to do so are like portholes in their hull causing financial losses, data breaches, systems intrusion, fraud and impair damage to reputation from these plots.

4.Future developments in the area

AI and machine learning tech will be more likely in the attackers' use to develop more authentic and personalized phishing campaigns that are more powerful and can thus not be detected by traditional detection methods. Establishing a phishing email or social media message which has been created by AI-powered language models that targets each individual using the person's language, writing style, and personality would make successful scams to appear more legitimate. And, deepfake technology, which uses AI to provide fake audio, video or images, can also be misused in social engineering that will involve impersonation of trusted persons or organizations.

With respect to the defensive side, machine intelligence and machine learning will be no less important in that they will be used to create more advanced phishing detection systems, which can be able to adapt and learn from new attack patterns. On the flip side of the coin though is the fact that the use of the adversarial AI techniques by attackers to bypass these AI-based detection systems will create the everlasting arms race with no end. Consequently, the multi-tiered defense mechanism incorporating AI security tools, user awareness training, and tight access regulation together with the well thought-out incident response planning will be a must for organizations to cope with phishing and social engineering development down the road.

4.1 Exploitation of Quantum Computing

With quantum computing technology wil develop, information can easily be stolen due to the possibility of hackers using the high computational power and break traditional encryption methods used. This encourages a new kind of phishing attempts that can focus on decrypted data, even if it is of an encrypted system. Some studies by IBM and NIST National Institute of Standards and Technology (NIST) brought up the issue of the consequences of quantum computing on the encryption algorithms and necessity of quantum-resistant algorithms [12], [13].

4.2 Artificial Intelligence for Phishing Detection Evasion

As AI and ML can be used by cyber thieves to create phishing attacks that can trick the traditional detection algorithms, so they are becoming more accurate. The complex attacks that can be designed to defeat both email filters, antivirus sofware and other security measures are being developed on a daily basis, having capabilities of constant adapting and changing. Studies by Microsoft and Cisco are conducted to test the machine learning adversarial techniques of bypassing phishing system detection [14], [15].

4.3 Exploitation of Emerging Technologies

This may pave the way for the newest trend of scamming and social engineering deception back into cybersecurity, but cybercriminals might outsmart the systems and conduct the attacks throughout the whole Metaverse including Web3 and DApps. Virtual environments shapeshifters, malicious smart contracts or perverted DApps could mislead the victims to steal information or crypto currencies. The security concern over tomorrow's technological level is still being investigated (Reports by Kaspersky Lab and Trend Micro) [16], [17].

4.4 Abuse of (IoT) and (OT) Devices

The growing tie of IoT and OT systems in industrial and critical infrastructural settings may attract cybercriminals who look to do phishing and social engineering attacks on them. Such microchipped devices could be misused as a pathway for malware distribution and information collection without the owner's permission. There are different types of attacks that the attackers can exploit the IT and OT devices through social engineering and phishing [18],[19], as Fortinet and Palo Alto Networks demonstrated.

4.5 Exploitation of Voice-based Interfaces and Smart Assistants

With the proliferating voice-based interfaces and smart assistants, the hackers may use them as channels for phishing and social engineering attacks. Voice Morphing, malicious voice commands or even smart assistant hijacking could be used to fool the users and make them send their sensitive Information or do the act that they don't intend to do. "Research by Amazon and Google [20], [21] into the vulnerability of voice-based interfaces and smart assistants" has also been conducted.

4.6 Targeting of Cloud-based Services

The proliferation of virtual jobs as well as cloud computer systems could make cybercriminals concentrate on those areas and take advantage of potential security gaps when trying to conduct phishing and social engineering activities. Attacks may be directed at workers remotely by means of fake video conferencing links or malicious applications which are cloud based. Research of Microsoft and Barracuda Networks have studied security issues with remote work and cloud services, such as phishing and social engineering, particularly. [22] [23].

Conclusion

The constant development of phishing frauds and exploitation technologies has been the greatest problem information security professionals, orginizations and the individuals in general have to deal with so far. What began as a naive (above definition) attempt at stealing email information through AOL users has reached the level of complexity, which takes advantage of multiple methods and sophisticated tools.

The process used by these schemes was initially limited to sending out fraudulent emails that pretend to be created by real companies in order to obtain personal and financial data. At the early stages, these heists were concentrated on certain online banking platforms and e-commerce sites. Nevertheless, as technology improved, they started to target any platform that was online. Attackers kept widening their spectrum of influence as social engineering like pretence and imitation took a toll and they successfully made attempts to titillate human psychology by tricking victims to disclose private information.Today, phishing and social engineering attacks are multi-channel ones, which include various routes such as emails, text messages, and social networks. The number of checkpoints significantly increases the efficiency of their attack.

New challenges such as the application of AI, deepfakes, and usage of new technologies, emerge due to the development of the new technologies which makes it difficulty for the detection and elimination of these problems.Then, also, you can apply different methods like behavioral analytics and biometric technologies which strengthen authentication processes and successfully detect the potential threats using the users' behavior patterns.

References:

[1] S. Furnell, "Phishing: The Past, Present and Future of Deceptive Communications," IEEE Security & Privacy, vol. 16, no. 3, pp. 76-79, May/June 2018.

[2] S. Furnell, "From the Phishers' Trenches," IEEE Security & Privacy, vol. 16, no. 5, pp. 80-83, Sep./Oct. 2018.

[3] N. Mitnick and S. Simon, "The Art of Deception: Controlling the Human Element of Security," IEEE Security & Privacy, vol. 1, no. 4, pp. 76-77, July-Aug. 2003.

[4] M. Jakobsson and J. Ratkiewicz, "Designing Ethical Phishing Experiments: A Study of (ROT13) rEAd&PHREAKxi;CYRIllIC/HACKoP, Unicode, and Roller Coaster Attacks," IEEE Security & Privacy, vol. 4, no. 4, pp. 40-47, July-Aug. 2006.

[5] M. Akwue and P. Hurley, "Advanced Persistent Threats: A New Reality," IEEE Security & Privacy, vol. 12, no. 5, pp. 18-21, Sept.-Oct. 2014.

[6] R. Deraison and S. Pillitteri, "Phishing and Social Engineering: Are You Vulnerable?," IEEE Security & Privacy, vol. 17, no. 4, pp. 89-92, July/Aug. 2019.

[7] P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "Protecting people from phishing: the design and evaluation of an embedded training email system," in Proceedings of the SIGCHI conference on Human factors in computing systems, 2007, pp. 905-914. [Online]. Available: https://doi.org/10.1145/1240624.1240760

[8] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2010, pp. 373-382. [Online]. Available: https://doi.org/10.1145/1753326.1753383

[9] IEEE Computer Society, "Cybersecurity Awareness and Training," IEEE Computer Society, 2021. [Online]. Available: https://www.computer.org/publications/tech-news/cybersecurity-awareness-and-training.

[10] R. M. Lee, D. Zand, and P. C. Litan, "Phishing and Social Engineering: Hacking the Human Element," IEEE Security & Privacy, vol. 19, no. 2, pp. 68-73, March/April 2021.

[11] S. Sharma and S. Bhatia, "Social Engineering: A Psychological Attack," IEEE Potentials, vol. 38, no. 5, pp. 18-23, Sept.-Oct. 2019.

[12] M. Campagna, "Quantum safe cryptography and security: an introduction, benefits, challenges and next steps," IEEE, 2015. [Online]. Available: https://www.ieee.org/publications/books/quantum-safe-cryptography-and-security.pdf

[13] Y. Shi, "Quantum computing and security: a new era," IEEE Security & Privacy, vol. 18, no. 4, pp. 16-22, Jul/Aug 2020.

[14] A. Drichel, S. Katzenbeisser, and M. Stamminger, "Adversarial deep learning for phishing detection," in Proc. 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Sep. 2021, pp. 260-269.

[15] K. Sriram and S. Iyengar, "Adversarial machine learning for phishing detection," Cisco, 2021. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/security/adversarial-machine-learning-for-phishing-detection.html

[16] K. Kuzin, "Metaverse: cyberthreats and security challenges," Kaspersky, 2022. [Online]. Available: https://www.kaspersky.com/blog/metaverse-cyberthreats/47873/

[17] S. Mehta and M. Anand, "Decentralized Finance (DeFi) and the Rise of Crypto-Crimes," Trend Micro, 2022. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/decentralized-finance-defi-and-the-rise-of-crypto-crimes

[18] Fortinet, "Securing Operational Technology (OT) Environments," Fortinet, 2021. [Online]. Available: https://www.fortinet.com/resources/whitepapers/securing-operational-technology-environments

[19] Palo Alto Networks, "IoT Security: Understanding the Cyber Risk and Mitigation Strategies," Palo Alto Networks, 2022. [Online]. Available: https://www.paloaltonetworks.com/resources/whitepapers/iot-security-understanding-the-cyber-risk-and-mitigation-strategies

[20] S. Zhang, N. Huaman, A. Bhardwaj, and B. Y. Zhao, "A study of voice attacks on mobile intelligent personal assistants," in Proc. 2021 USENIX Annual Technical Conference (USENIX ATC '21), Jul. 2021, pp. 425-440.

[21] A. Kizhner, G. Krishnan, and S. Sengupta, "Security and privacy of voice assistants," Google AI, 2021. [Online]. Available: https://ai.googleblog.com/2021/07/security-and-privacy-of-voice-assistants.html

[22] Microsoft, "Remote work, cloud security and the rise of phishing attacks," Microsoft, 2022. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2022/03/24/remote-work-cloud-security-and-the-rise-of-phishing-attacks/

[23] Barracuda Networks, "Threat Spotlight: Phishing in the Cloud," Barracuda Networks, 2021. [Online]. Available: https://www.barracuda.com/cloudgen/wp-content/uploads/2021/04/Threat-Spotlight-Cloud-Phishing.pdf