Sri Lanka Institute of Information Technology

BSc Honors in Information Technology

Specializing in Cyber Security

Introduction to Cyber Security - IE2022

ICS Assignment-Individual

W.V.A. MENDIS

IT23236028

PHISHING ATTACKS

Table of Contents

ABSTRACT

Phishing is a type of cybercrime in which the perpetrator pretends to be someone trustworthy in order to dupe the victim into divulging information such as their username and password or even their banking details. Such attacks are primarily underlying emails, chat services, or fake web pages aimed at getting the victim to open a malicious link or download a threat malware. There has been an increase of sophistication and plausibility of the above techniques as they are more personalized these days than they were in the past.

Different types of phishing mechanisms are present including spear-phishing which is where individuals or organizations are targeted and whaling which targets high profile individuals such as chief of the executive officer. With fake emails or calls being a prominent feature of phishing attacks, their effectiveness is a cause for concern on the security of individuals, given that it may lead to personal information being accessed, funds lost, and corporations facing problems arising from a data leak. Some of the measures in place to mitigate phishing attacks include educating users, availing multi-factor authentication, and other activities such as email filtering.

The application of these measures is reasonable and increases as time goes by and the trends in phishing attacks evolve. Raising public awareness and establishing more effective detection systems in the cyber space are extremely vital in the 21st century in the fight against cybercrimes that are aimed to cause less damage to companies than before like phishing

INTRODUCTION

In the present-day digital world, the fishing threats are considered some of the most common and even harmful crimes today. Well, in simple words, it is a 'con' game played by criminals pretending to be someone they are not, for instance, banks, popular websites, or even government agencies in order to extract personal information such as a person's password, credit card information, or social security number. Phishing is therefore not limited to emails and it can be encountered through text messages, phone calls and even social media making this quite a flexible and wide-ranging danger. In the criminals' world of the internet, where everything is conducted online, such form of manipulation has proven to be their greatest weapon.

Phishing is a particularly malicious type of attack, because it is based on social engineering. Unlike cyber hacking, many phishing attacks do not involve any known technical weaknesses but instead rely on basic psychology manipulating emotions, such as fear and urgency, to encourage the victim to act without confirming the legitimacy of the communication. Consequently, such strategies can render even the most powerful technical solutions useless; after all, the most sophisticated system may become compromised thanks to a single operative's blunder, incurring financial, informational and personal data losses.

To add on, the issue of phishing has also become rampant with medical scammers utilizing the new health conditions. With attacks becoming pandemic, even organizations are targeted as phishing is used to either exfiltrate valuable organizational information or even carry more sophisticated malware attacks such as ransomware. The increasing complexity of phishing means that there are calls for stronger defenses such as the implementation of user training and awareness programs, as well as the active monitoring of the threats for the sake of alleviating their impacts.

EVOLUTION OF THE TOPIC

History Of Phishing attacks

In the early-***1990s***, dial-up internet access was available for free, but those hesitant to pay used a 30-day free trial via an AOL floppy disk. To continue accessing the internet, scammers disguised themselves as AOL administrators and phished for login credentials. As internet usage increased, they accessed users' accounts and sent spam.

A look at the history of phishing reveals that the first phishing email is thought to have originated sometime around the year ***1995***. The first many knew of the existence of phishing was five years later when the Love Bug struck.

The development process of phishing and cybercriminal activities, on the other hand, has its own timeline with important events. In ***2001***, because of the upswing in e-commerce, conspirators laid out imitation pages of legitimate sites such as eBay and PayPal amongst others. Two years later in ***2004***, hackers started using pop-up windows that sought to obtain sensitive data, information and techniques like spear phishing, smishing, and key logging became popular. The introduction of Bitcoin in 2008 proved a sweetener for cyber criminals as its Article allows payment for illegal services with greater safety and has given rise to the development of better malware.

By ***2013***, it was reported that the evolution of ransomware epidemic was using phishing which was much more efficient and posed more danger to users. In ***2017***, hackers began to use HTTPS on their spoofed websites in order to make the sites seem more authentic. This phenomenon was observed in ***2018*** as well when cybercriminals began to include viral codes in graphic images to escape antivirus detection. By ***2019***, better yet, gift card phishing schemes became more sophisticated as the participants were promised rewards and threatened with consequences for not meeting the requests of gift cards or cryptocurrencies.

The importance of phishing awareness has increased in both personal and professional settings, with phishing attacks among businesses rising from 72% in 2017 to 86% in ***2020***.[11]

How Does Phishing Attacks Work?

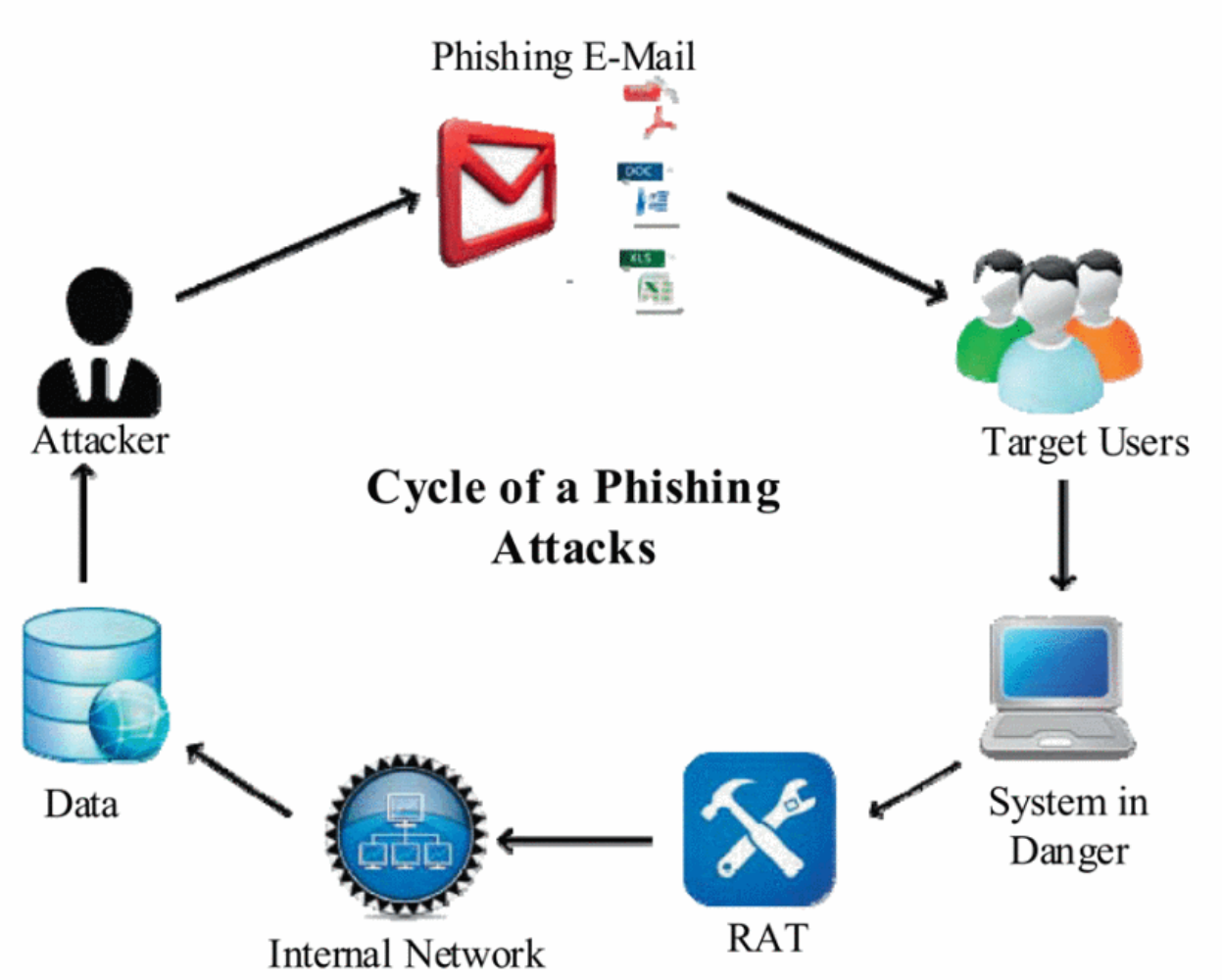
1. **Bait**
   In this phase, the attacker creates a fake but compelling message as though from a reliable individual, say a bank, company, or online service. Such a message is often transmitted via email, SMS, text messages, or social networks and is likely to look real. Its effects are to capture attention and make the recipient believe that they need to act fast, often appealing to one's sense of fear or breach of curiosity.

2. **Hook**
   The said message contains an actionable item to be followed, which may include clicking on a link, opening an attachment, or submitting personal information like passwords. The attacker is usually in a hurry, stating that the victim's account is at stake or that something needs to be done right away and without failure. This way the victim is provoked into acting, without being able to assess the request to the full extent.

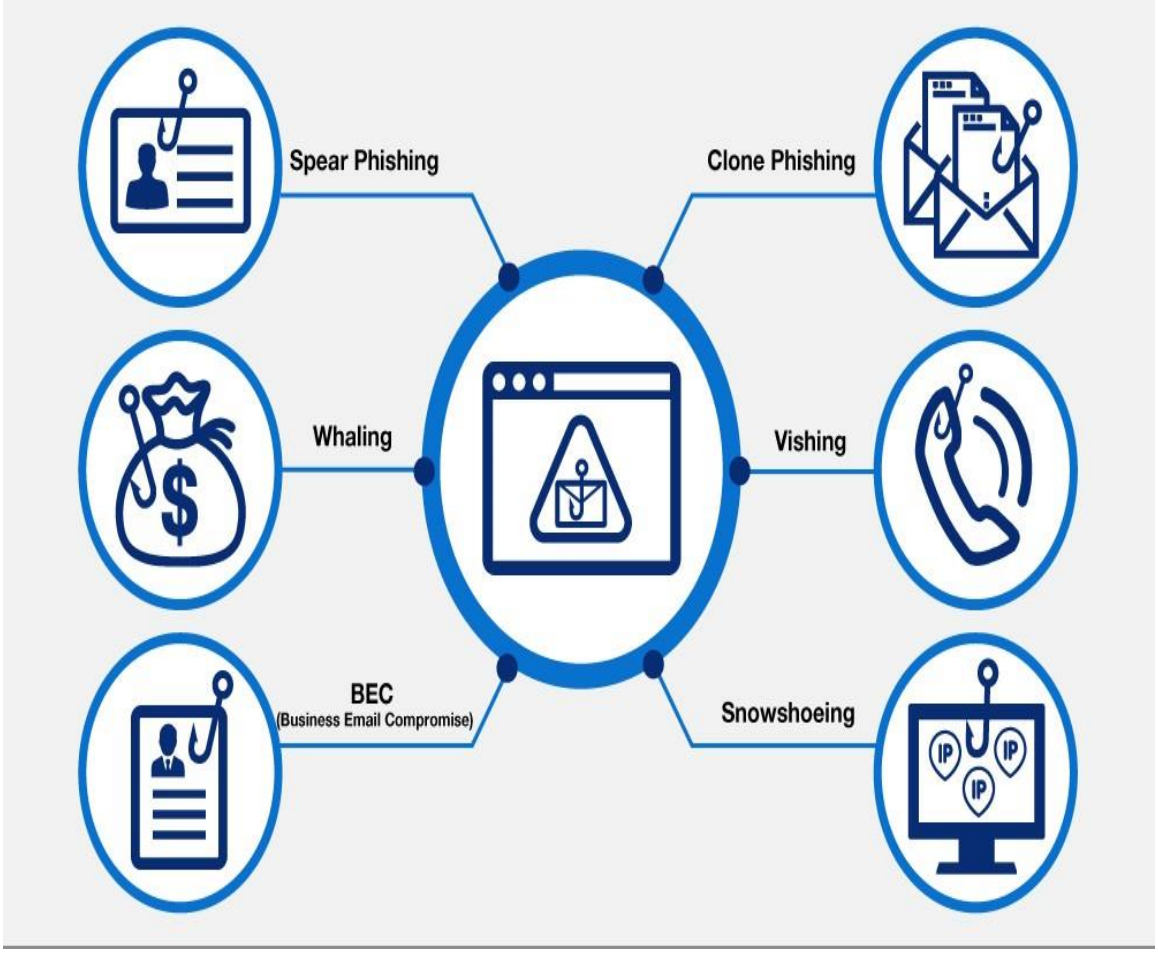
3. **Deception**
   After clicking the link or carrying out the instruction that the victim had been provided with, they land on a spoofed site that looks exactly like the real one. At this point they are requested to enter some personal sensitive data like log in details or their card details. The attacker apparently goes to great lengths to make it look like the site is genuine in order to put the victim at ease.

4. **Data Harvesting**

After the victim provides the information, the attacker steals the information for his own benefit. And the stolen data might help in committing identity fraud and even in accessing the victim's banking services perpetrating transactions without their consent. Usually, the victim does not know that she has been compromised until the data that was stolen is put into use, hence why phishing is a sophisticated and destructive act.



Types of Phishing Attacks



1.Spear Phishing

What is spear phishing?

Spear phishing is a subset of phishing that is aimed at individuals or groups within an organization. It is a very effective form of phishing, a deceptive practice that employs emails, social networking, instant messaging and other means to trick people into giving up sensitive information or undertaking any behavior that will lead to a breach, loss of data or even money. Phishing tactics are designed in such a way the attacks can be carried out without necessarily knowing the victims by spraying a combination of messages, however with spear phishing attacks there are always specific targets and these attacks have to involve some research.

Of course a spear phishing attack would entail an email and also an email attachment. The email contains information pertaining to the target such as their name and position within the organization. This social engineering strategy increases the likelihood that the intended victim will perform all actions required for any successful infection, such as opening the email as well as the email attachment.

Prevent and Mitigation Spear Phishing

Phishing attack prevention and mitigation strategies consist of both technological and behavioral factors. Organizations and individuals can undertake the multi-layered security mechanism known as **multi-factor authentication (MFA)** to ensure that there is no easy access to the systems, even though the credentials have been accessed by malicious users. Email filtering software is designed to filter out unwanted and potentially dangerous communications, while also reducing the risk of operating systems and applications out of date which is a welcome opening that phishing attacks can exploit. User education is equally important to this teaching people to look for things like the correct sender address, grammar, or links to click on dramatically reduces the risk. Moreover, organizations should conduct phishing simulation exercises for employees so that they know how to counter the threat. Backing up important information is also a helpful practice in order to lessen the consequences when an attacker infiltrates the systems successfully.

- Security awareness training
- Controls for identity and access management
- Controls for cybersecurity

2.Whaling

What is whaling?

Whaling is a type of phishing attack which aims at high-ranking individuals in an organization for the purpose of obtaining confidential resources or performing transactions that are not legitimate. Such complex attacks tend to involve details of the individual who is targeted, and many times people impersonate their colleagues or bosses. The risks associated with the success of such a whaling campaign include loss of funds, breach of confidential data, and tarnishing the reputation of the firm.

In order to counter such threats, resources of an organization should include the adoption of other security protocols such as multi-tenancy, email filtering, education and training of users and employees on the precautionary measures to avoid attack in such use of advanced social engineering techniques.

Prevent and Mitigation Whaling

Whaling is a specific form of phishing that is directed at high-level executives and management in a particular organization. It involves both technical and human measures for prevention. High management should employ **DMARC, DKIM**, and **SPF** protocols, conduct regular security awareness training, implement Multi-factor authentication, and add verification measures for large sums of money transfers. Following the attack, focused Damage Control a strong incident response plan should be in place in addition to a network segmentation policy so there are as few access points to sensitive information as possible. Monitoring and auditing of activities related to communication and the movement of finance on a 24/7 basis can also lessen the threats and help contain the effects of whaling.

- Data Encryption
- Regular Security Audits
- Secure Email Policies

3. Business email compromise[BEC]

What is BEC ?

The Business Email Compromise (BEC) is a kind of phishing attack which is centered on a particular individual such as an executive or a finance manager with the power to sanction payments or gain access to crucial details. Key in the practicing of BEC is capping, which entails the use of an email address that has either been faked or that looks like the trusted source's email address to send an appeal as a high-ranking officer or a business associate. These types of attacks are always economically motivated, with the primary aim being to swindle the victim in charge to wire transfer huge amounts of money to bogus accounts. In the other cases, con artists' intent is to gather internal business, or log in information, compromising even deeper into the security of the organization. The effort and tactics involved in BEC identity deception makes it one of the most expensive as well as damaging attacks to an organization considering the level of phishing rogues.

Prevent and Mitigation BEC

In order to mitigate risks associated with Business Email Compromise (BEC), there is a need for a trifecta of technical measures, awareness amongst employees, and hardline policies within the organization. On one hand, the introduction of **DMARC, DKIM**, and **SPF** protocols, otherwise known as email authentication protocols is likely to discourage instances of email forging. Another preventative mechanism is the use of **multi-factor authentication (MFA)** where additional features are included in the access of sensitive systems and emails enhancing security.

Another significant and basic strategy is ensuring regular and effective security awareness training in assisting employees in identifying phishing attacks and the dangers of BEC. Moreover, it is important that outsourcing firms put in place rigorous verification procedures for any payment instructions or amendment of banking details including requests for the transfer of funds or confidential information always being authenticated via several means i.e. telephone calls. Finally, there should be regular monitoring and auditing of email use especially by vulnerable individuals, such as senior management, which may identify irregular behavior and decreases the chances of a successful BEC.

- Multi-Factor Authentication[MFA]
- Regular Software Update
- Use of Encryption

4.Clone Phishing

what is Clone phishing?

When discussing clone phishing, it refers to an email-centric approach where the attackers recreate genuine emails of trusted groups, except for the fact that they come with harmful links or attachments. Such imitator emails tend to be almost naively identical to the original with the aim of deceiving the users that they are original. Tactics in clone phishing are use of running offers in the emails or recently updated ones. In most cases, however, such messages nigger presumes include internet connections to targeted malwares or malwares attached like those of torsion type such as ransomware. The people most susceptible to such con attacks tend to be those who do a lot of online banking or shop on major sites like amazon. Thus pay close attention to the design or the compelling of the email's senders address to avoid dangerous con email clones.

Prevent and Mitigation Clone phishing

Must preventive and responsive measures against clone phishing be multi-faceted encompassing technologies, education and organizational policies? Such measures are worth being put in place in that organizations should institute strategies like the use of email authentication protocols **DMARC, DKIM** and **SPF** aimed at validating embracing all incoming emails as a way of lessening the chances of hacking. Constant security awareness training is equally important as it enables the staffs to detect suspicious email messages and dissuades them from acting upon strange requests without cross checking through other means.

In addition to the above, a well-developed and tested incident response plans allows for timely response to threats in case an attack is successful, where the attack may be executed in spite of all previous preventive measures. In addition, regular Inhouse security audits and upgrading of email filtering mechanisms minimizes the risks by ensuring that potential threats do not get to users' mailboxes. Lastly, the use of endpoint protection solutions can enhance security by providing means to handle malware that can be downloaded from compromised emails.

- Educate Users
- Verify Sender Details
- Limit Email Permissions

5.Vishing

what is Vishing?

Vishing ,otherwise known as ***voice phishing***, refers to a telephone-based cybercrime where victims are coerced over the telephone to provide their secret information- credit card, pin numbers, and even passwords. Criminals often rely on impersonation of the victim's trusted contacts, be it banks, government offices or even technical assistance, employing social manipulation strategies involving emotional appeals of either urgency or fear. They might use robotic devices, or simply manipulate live persons promising threats or rewards in return for the victims' personal information. This is because vishing takes advantage of an individual's predisposed trust toward another person over the phone and is therefore so effective that it is recommended that people do not give out personal information when they have not validated who the caller is.

Prevent and Mitigation Vishing

The most effective way of combating vishing is through a two-pronged approach combining user education and implementing technology to secure the users. Both organizations and individuals must learn about appropriate vishing behaviors; for example, how requests to provide sensitive information over the phone, or requests to act immediately over the phone are common red flags. The use of tightening of controlled access barriers using caller ID verification tools can also mitigate the challenges posed by other more destructive forms of attacks.

Moreover, repeating these messages without providing information over the phone until the request is verified, for instance, by calling the organization requesting the information, could be beneficial. It is also advisable for institutions to put guidelines on what information can be solicited from quartered targets and hold preemptive measures aimed at preparing the employees to face the threats of vishing attacks. Finally, should an increase in the terms of threats be noted, reporting all such calls in sufficient detail should help improve the situation.

- Keep Information Quiet
- Never give remote computer access
- Always check phone numbers

6. Snowshoeing

What is Snowshoeing?

In the field of cybersecurity, snowshoeing refers to a spamming tactic via which spammers or phishers make use of numerous IP addresses or email accounts to spread their spam or phishing message to reduce the chances of its being flagged as spam. Sending out low amounts of spam from every source instead of high volumes of spam from one source enables many hackers to bypass those systems designed to block spam by obvious patterns. Thus, this method decreases the chances of the spam being treated as harmful, hence creating a more complex detection system. For effective suppression of snow shoeing, high level security measures accompanied by behavior analysis and reputation-based filtering have to be put in place in order to understand and protect against these geographically distributed attacks.

Prevent and Mitigation Snowshoeing

In order to avoid snowshoeing attacks, it is recommended to use a variety of technical means, as well as to educate users. Thus, organizations need to apply reputation-based filtering techniques to check the trustworthiness of the sources of incoming e-mail no matter what IP-and-domain or behavioral detection techniques to track people who seem to go against normal sending habits in an attempt to spam the inbox using various IPs. The use of email authentication protocols in particular helps in reducing the likelihood that forged emails (spoofed ones) are sent out.

Continual overhauling of course on employees on security training also has a very great role in raising problems awareness and controlling ‘forgot wits’ tendency in dealing untrustworthy e-mails. Owing to the above approaches, companies will be less exposed to snowshoeing and its impacts on their email systems; on the contrary, fewer spam and phishing attacks will be directed at them.

- Educate Uses
- Implement strong passwords
- Limit account lockouts

Effect of Phishing On Persons And Organizations

Effect of Phishing on Persons

In relation to individuals, phishing can prove costly in that it can result in illicit spending, impersonation or even fraud. When this happens, a person can easily lose their savings or even their entire bank balance or even excess debts on their credit cards, which will take a lot of time to restore those resources. The psychological effect is quite high; people also experience fear, shame, and sometimes anger, especially when they lose control over their private data. This often leads to depressive symptoms regarding this aspect, and therefore, one becomes careful when engaging in such activity in the future, thus lessening healthy optimism.

Phishing attacks are an ordeal to the victim as it entails a lot of activities like changing passwords, checking bank balances, and other precautions. These requirements are life-altering, bring more worries about safety of their information, and extend beyond financial implications, changing their views on online mechanisms.

Effect of Phishing on Organizations

Phishing has the potential to cause heavy financial losses for organizations, impairing their ability to make profits and reducing the efficiency of the day-to-day activities in the organization. Theft of financial data can lead to loss of money from the organization and costs incurred in responding to and recovering from the incident can be hard on the pockets. In addition, the organization may be forced to get more insurance acts and more advanced security measures after the attacks or incurring the attacks themselves. Often this increase is in(face) the possibility of sustaining regulatory sanctions in regard to costs associated with implementation of remediation costs.

Incorporated with phishing scams and other cyber activities come financial losses, humiliation, and even damage that hampers the confidence of customers forcing them to rethink their relationships. In this digital business age, customers are expectant of s e – security and avoidance of any risks. This may result in loss of brand loyalty and even opportunity costs incurred. Companies should be involved in cyber policing to mitigate the occurrences of such attacks.

Future Development In This Area

With advancements in technology, specifically their skills, attackers will increasingly adopt Artificial Intelligence and machine learning to execute sophisticated phishing schemes. The audio, and video manipulations, including social engineering techniques, will be aided by realistic deep fake functionality. To mitigate risks using machine learning, one will be required to implement the technology in developing anti-phishing solutions and in the devising of new threats. New problem arises while combatting the information thieves because exact same measures can be used in mitigating the impacts. The companies need to adopt a comprehensive security framework which addresses incident management, employee training, employs artificial intelligence robust solutions as well as restricts sensitive information access to authorized individuals only.

There are some developments in Phishing are mentioned in below.

1.AI-Driven Personalized Phishing

As time progresses and technology advances, particularly artificial intelligence, the evolution of personalized phishing utilizing AI will keep getting better. Due to machine learning approaches, cyber-terrorists will find it much easier to sift through large datasets and highlight particular individual weaknesses and likings. This extreme nearness of the target will make it easy and more difficult to detect the feature of targeting the victim, thus drawing the lines in between the rosy phishing and accepted

communications. Furthermore, the capacity or ability of AI to learn and improve means that phishing would also be in a position to improve at the same time making traditional security measures ineffective. Therefore the evolution of the threat would call for sophisticated measures of detection and prevention of these attacks.

2.Phishing via IoT Devices

As the number of smart devices connectivity in homes, companies and critical infrastructure increases, phishing through IoT devices is becoming one of the threats. In this case, systems that rely on the technique of phishing are coming into play. Hacking is equally useful, and these zombie networks of devices provide new avenues for hackers. Because most IoT devices have very weak security, they may serve as a good entry point for hackers looking to retrieve sensitive data. It is anticipated that with the further developments in this space, there will be advanced phishing attacks that take advantage of the close relationship between IoT devices and the end user's data making it difficult to detect malice. Additionally, the use of advanced technologies like ***artificial intelligence (AI) or machine learning (ML) systems*** increases the problem since such technologies may also be employed for more advanced and detailed attack scenarios on the target audience. These challenges can be mitigated by enforcing new safety measures and educating the public in the ways that do not allow for the IoT expansion to be faster than the protective measures that are designed for it.

3.Phaas[Phishing as a Service]

The trend of Phishing as a Service (PhaaS) will only grow and improve as PhaaS becomes a service, a model that hackers, well-known for their nefarious activities, have increasingly gravitated to. In the development of PhaaS it is likely that the better and more accessible servers will be created meaning that even an average internet user with little or no computer expertise will be capable of executing a phishing attack within the shortest time possible. Such systems may also include greater levels of automation, artificial intelligence, and other diverse attack methods which will make it much harder to separate spam and phishing from normal whitelisting restrictions. PhaaS providers are also likely to constantly improve their products in order to escape from new detection systems as well as engaging in social hacking differences controlled by technologies on offer will be different. For the reasons outlined above, the availability of such phishing services also indicates a shift towards particularized services which are likely to be less exploitable and more commercially oriented. In the face of the inevitability of continued growth of digitalized activities, PhaaS will still emerge as a lingering menace and thus will necessitate the need for measures such as strategies that are flexible and anticipative of the threats brought about by this rather unpleasant business model.

4.Deepfake-Enabled Social Engineering

Social engineering attacks conducted through Deepfakes are a growing concern and pose a threat that is only likely to increase with the advancement of deepfake technology in the future. As an increasing number of years evolves, the creation of such synthetic media that can resemble a human being, right down to its finest details, will assist evil people in drastically changing the nature of human interactions. Trust in communications over digital platforms, or the inter-communications of contacting parties, will be shaken as individuals such as authoritative personnel or counterparts will be impersonated using deepfakes instantly above the target of contact. This would make it easier to execute more effective phishing attacks that could cause serious personal, organizational, or even national security breaches. With the pervasiveness of such artificial intelligence and deep learning devices, it will even get worse since people will not tell the difference anymore between what is fake and what is the reality. As the use of deepfake applications will become common and their recognition by the opposition will be very challenging, the conventional methods of authentication and validation will not be effective anymore and therefore new strategies will have to be designed and the situation managed to control the social engineering threats posed by the deep fakes and other such technologies.

5.Mobile App-Based Phishing

Phishing using mobile applications is emerging as a concern with potential threats which scheming users through mobile applications. With the consistent increase in smartphone and application , phishing in these platforms has also become more sophisticated. In the coming times, mobile apps will be difficult to use without detection even with the help of artificial intelligence and machine learning designed to help the perpetrators of such offenses to plan better and targeted attacks. Also, as some applications will be integrated more closely into such services as banking and healthcare the harm of successful phishing attacks will increase. With many mobile users enabling apps to access private information or sensitive data the risk of being able to expose that information is enormous. In light of this trend, focus in the future could be directed toward app store security, users training, and anti-phishing strategies that would help contain known threats within the app stores.

How to prevent phishing Attacks?

1.Exercise extreme vigilance with emails and messages

Review most attentively any received email or message, and especially those which are from unfamiliar and/or unanticipated sources. Additionally, do not access any linking pages or files if an individual is not confident about their authenticity. Such mail would be phishing solicitations seeking for an audience but rather inducing a temporal effect or even pretending to be some famous organization. But first and first, you should seek adequate verification of rein to execute one's intent respecting the methods .

2.Always hover at the appropriate points before clicking any link

As you fill in the information, kindly do so only if you have analyzed the right google address to use. Ensure you only visit the secure and intended website that starts with 'https://' there is no other site for that purpose. Phishing disguise themselves providing fake domains that are already familiar to the would-be victim. Hence checking the validity of the given URL helps one not to fill any forms in a phishing site that is only designed to collect people's information.

3.Enable MFA options

Besides, the browser is discouraged from relying on the password as the abode of security with the introduction of multi – factor authentication. With Multi – factor authentication for example at the point of log in a second code has to be verified usually through a mobile phone. This is a great enhancement since in cases where the login credentials are compromised, the account is still challenging to access.

4.Make sure your programs are current

Regularly modify the operating systems as well as applications and also antivirus systems to provide protection from the attacks based on threats that have been made public. In most cases, the enhancements of the software updates are in the form of anti-intrusion supplements to curb any weaknesses that could be exploited by the attackers. More so, the management by extension of such turns to the unitary form practices helps in curtailing the risk of a situation occurring such as being behind schedule.

Conclusion

As a conclusion, attacks carried out using phishing is a persistent and growing threat to individuals as well as organizations. Cybercriminals constantly modify their strategies making it highly imperative to provide security measures, educate end users and create an awareness. Men should be on the lookout for questionable messages while women include implementing the best strategies to prevent risks including security measures for the organization and education of the employees Base on the recent attack that took place within the organization and the three management strategies adopted, there is no doubt that phishing attacks can be prevented and the private information of clients and employees safeguarded through the promotion of cyberspace culture and the employment of high level of protection technologies. There is a need for such actions and partnership between the players, on this complex problem, because it is a very important and persistent challenge in the virtual space.

References

Introduction

https://cofense.com/knowledge-center/history-of-phishing/

https://vpn.sliit.lk/proxy/20cf04a6/https/ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9461272

History of Phishing Attacks

https://www.verizon.com/business/resources/articles/s/the-history-of-phishing/

https://en.wikipedia.org/wiki/Phishing

https://cofense.com/knowledge-center/history-of-phishing/

https://www.getcybersafe.gc.ca/en/resources/history-phishing

How Does Phishing Attack Works?

T. N. Chitti, A. Pandey, B. K, D. B. S and H. Rusiya, "Mitigating Online Fraud: Understanding Phishing Threats and Prevention Strategies Using Machine Learning," *2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, Chennai, India, 2024, pp. 1-6, doi: 10.1109/ICONSTEM60960.2024.10568657.

https://vpn.sliit.lk/proxy/20cf04a6/https/ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10568657

https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/

Types of Phishing Attacks

//spear phishing

======what is spear phishing

https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing

https://vpn.sliit.lk/proxy/42245fb3/https/ieeexplore.ieee.org/document/8300257

=======Prevent and Mitigation Spear Phishing

https://www.ibm.com/topics/spear-phishing

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8821758

//whaling

======what is whaling

https://www.ibm.com/topics/whale-phishing

=====Prevent and Mitigation whaling

https://www.bitsight.com/blog/what-is-whaling-attack-prevent-it

// Business Email Compromise[BEC]

=====what is BEC

https://www.cloudflare.com/learning/email-security/business-email-compromise-bec/

===== Prevent and Mitigation BEC

https://staysafeonline.org/resources/business-email-compromise-what-it-is-and-how-to-prevent-it/

//Clone phishing

=====what is Clone phishing

https://us.norton.com/blog/online-scams/clone-phishing

===== Prevent and Mitigation Clone phishing

https://www.linkedin.com/pulse/what-clone-phishing-prevention-solutions-your-business-amit-birk-lqpkc

//Vishing

=====what is Vishing

https://www.fortinet.com/resources/cyberglossary/vishing-attack#:~:text=Vishing%20Attack%20Definition,to%20gain%20a%20financial%20advantage.

=====Prevent and Mitigation Vishing

https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/vishing-attack/

https://vpn.sliit.lk/proxy/42245fb3/https/ieeexplore.ieee.org/search/searchresult.jsp?newsearch=true&queryText=vishing

//Snowshoeing

=====what is Snowshoeing

https://www.paubox.com/blog/what-is-snowshoe-spam

https://vpn.sliit.lk/proxy/42245fb3/https/ieeexplore.ieee.org/document/8406222

=====Prevent and Mitigation Snowshoeing

https://ctemplar.com/what-is-a-snowshoe-spam-attack-and-how-to-prevent-it/#:~:text=To%20avoid%20your%20legitimate%20email,your%20email%20as%20snowshoe%20spam.

Future Development In This Area

https://thesecuritycompany.com/the-insider/what-does-the-future-of-phishing-attacks-look-like/

https://cybersecurity-magazine.com/phishing-in-2024-heres-what-to-expect/#:~:text=AI%20technology%20is%20revolutionizing%20phishing,personal%20communication%20styles%20and%20preferences.

How to prevent phishing Attacks

https://vpn.sliit.lk/proxy/20cf04a6/https/ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8550910

https://www.cloudflare.com/learning/email-security/how-to-prevent-phishing/