BULLET: Jurnal Multidisiplin Ilmu
Volume 3, No. 05, Oktober-November (2024)
ISSN 2829-2049 (media online)
Hal 696-712

An Analysis of Phishing Attacks: Information Technology Security: Cybercrime and Its Solutions

Noman abid

American National University USA

nomanabid12345@gmail.com

Abstract

Phishing is one of the most primary and persistent threats when it comes to cybersecurity, and is grounded on deception tropes which try to pry information from individuals or organizations or get unauthorized access to their systems. Phishing, which is discussed in this review, circles around every trick the criminals employ, the collection of intelligence by the attackers and the countermeasures which may be applied to contain the attacks. There are different types of phishing such as spear-phishing, phishing have become popular so have AI-based attacks which shows that one method is not sufficient anymore. The organizations hence need to implement several layers of defense like; Information user awareness, two-factor or multi-factor technique, superior email filtering technique and rigid enforcement of the email verification procedures like SPF, DKIM and DMARC. New chances will be expected from the methods like Machine Learning, Behavioral Biometrics, and Block Chain for efficient detection and control of the phishing. Zero Trust security model, which only periodically validates each access request to reduce the vulnerability of successful cyber-attacks has notes on how to use it. Likewise, there is more sharing of intelligence and working across industry in real time very central in tackling phishing threats. At present, there is a heightened appreciation of better user security, the dangers that require anticipative measures, continuous monitoring, and popularity of use. This paper emphasizes that combat against phishing requires a systematic and timely approach that incorporates technology and user awareness as well as organizational backing. As with the assistance of following what has been described here as best practices and solutions, one and everyone and every company may decrease the probability of being spoofed and the consequences of such spoofing.

Keywords: Phishing Cybersecurity, Multi factor Authentication, Email Filtering, Spear-phishing, AI-driven Attacks, Behavioral Biometrics, Zero Trust, Microsoft, Email Authentication, Machine Learning, Block chain Crime, Threat Intelligence, User Education, Phishing-as-a-Service.

INTRODUCTION

Phishing scheme is another type of cybercrime which is aimed at making people surrender their passwords or any other credentials, personal and/or financial data to the attacker. Phishing is one of the most known and evolving cyber threats types, with phishing remaining as the preferred technique by cybercriminals to gain access to IT systems, networks, and accounts. As the authors of this paper reveal, phishing attacks that have recently emerged are still a threat to users and firms worldwide. The name ‘phishing’ has been derived from the term ‘fishing, this is so because the attacker is in fact fishing for potential victims. The attacker initially emails a victims with a disguised phishing message that includes the look and feel of a customer’s genuine company, bank, email service, government agency or any organization with which the victim is likely to transact, in order to ‘hook’ the victim into replying or performing an action that compromises the victims security [1]. There is email, which is referred to as phishing, phone calls which are called phishing, sms which is called smashing and, at last, social sites by using social engineering techniques.

Many of the attempts at phishing are made in campaigns, in which the attacker transmits multiple messages to several prospective targets. It focuses on building a person’s trust and seeks to deceive that person or tempt him/her (For example, a warning of a suspicious account, or an offer of win in lottery, or an employment opportunity), or appeal to the person’s sentimentality (for instance, an urgent, desperate need for cash) [2]. Their advantage comes from social engineering – psyche of the attack lays in understanding the simple notion that the victim will trust the organization that contacted him/her and inescapably will catch on the sense of urgency or dishonesty of the letter. Such attacks are wife and hazardous especially for individuals as well as companies. In the case of personalities, for example, participation in the phishing releases prompts monetary damage, stolen identity, and privacies violation. But for organizations it can go further and wider because people do work not individually but in groups. Phishing is relevant to be mentioned as it serves often as the initial stage for further attacks, for example, with ransom ware, theft, or the corporate network of a business. Following a successful implementation of a phish attack, companies face the following risks such as; Financial loss Legal/Regulatory repercussions Reputational

loss For example, the loss of customer data or a security compromise resulting from a phishing attack will mean that a firm will lose its customers [3].

To mitigate the impact of phishing, organizations have put in place the following measures among them; Technical Control Measures; these are measures taken to counter the problem of phishing; they include; spam filters, Secure email gateways, Multi-factor authentication among others. Nonetheless, the technological barriers enough and in an efficient way cannot dissociate the threat of phishing attacks. Phishing is one of the most effective types of hacking, which is used taking into account people factor and, unfortunately, the absence of which is still a crucial factor in such cases. Thus, security education and training help users to develop a practical possibility to prevent Phishing attacks [4]. Many establishments have incorporated annual or semi-annual phishing attacks, and sensitization campaigns as a way of informing employees about penalties for phishing and how to avoid the tricks. Phishing today as a subsistent method of cyber-attacks is dynamic because it thrives well in change of different technology controls; new trends emerging today include spear-phishing (point and shoot) and whaling (attacking the big fish).

They are also using better Implements such as Artificial Intelligence and Machine Learning to increase the effect of the attacks. Schtch dynamic ensures that phishing remains as active and versatile threat that will continue to affect the organization and the individuals. Phishing is an essentially toxic phenomenon that has begun to evolve in the field of cybersecurity, and its distinguishing feature is a lack of a sufficiently comprehensive approach to combating it. Despite the fact that there has been a decrease in the incorporation of advanced technology in cyber-criminal activities, the element mentioned above, Phishing risk is steadily on the rise owing to their human aspect. This shows the continuous dynamic nature of the human attackers it becomes necessary that peoples and organizations are well equipped to always change with the changing phenomena within the phishing domain in both technical and social facets [5].

TYPES OF PHISHING ATTACKS

To its class, phishing is not homogenous; it is not something that is ricocheted in an equally homogenized manner. Recently, hackers have produced new and developed types of phishing to fulfil one or the other objective and target specific persons, companies or systems. This knowledge enables one to treat the problem of these threats in the future, given the understanding of the various types of phishing. This section concern with the details of now and near future of phishing attacks according to the type which found to be most common [6].

Email Phishing: The first one and also the most apparent type of phishing is the email phishing. In these attacks, the actual crooks send others messages that look like they come from friends and related organizations such as banks, governmental bodies or other well-known companies. Such emails are normally of higher sense of urgency and include links that users are urged to click, file attachments that are urged to download or other information in fake sites. The ultimate goal of using email phishing is often to extract the login details, payments or individual details from the victim [7]. However, in the present time, with the help of nothing but email filters and anti-phishing tools, email phishing is a very efficient form as it requires very less effort for the attacker.

Spear Phishing: Spear phishing is less like phishing by concentrating on a particular person or organization in the targeted section. While in the case of mass email phishing, the e-mail is sent to numerous and unrelated people and passersby, in the case of spear phishing, it is attempted that any possibly obtainable information about the intended target is gathered, preferably from social networks, the target's website and or previous communications. Luckily, this level of tailor made increases the chances that the victim will fall for the trick. For instance an attacker may dress as a staff, manager or supplier and send an email that appears to come from the imitated identity and informs the target that she/ he needs to release information, money etc Spear phishing is thus far more risky than the normal form of phishing since the latter invests time and tries to manipulate details known about the target [8].

Whaling: Spear phishing is a form of whaling, and it is directed at directing its assault on senior employees or any employee of high standing within an organization. Because these people get hold of sensitive corporate information or financial information, the threats of whaling attack are way higher. The emails and messages used in whaling attacks are, therefore, mostly very sophisticated, and are framed in a manner relevant to the target's position, for example a request to make a wire transfer of large sums of money, or to approve an important business transaction. Just because any of these individuals gets a hold of it, whaling attacks can mean massive fund embezzlement as well as reputational destruction of an organization [9].

Vishing (Voice Phishing): Vishing is the exact equivalent of email phishing, but it is done over the telephone; in a conversion. In most cases, the attacker simply impersonates a legitimate third party including the bank or government, and then gets the potential victim to surrender his or her password, credit card number or Social

Security number. Vishing is also done through a phone call, left voice message or an instant message from the robocalls. These forms of attacks are not only based on using the most immediate messages that will compel the victim into doing something but also threat messages [10]. Althouth vishing is not as widespread as email phishing, it is as efficient when the attacker uses social engineering to gain confidence in the target.

Smishing (SMS Phishing): Smishing on the other hand means phishing through text messages or the short message service (SMS for short). Smishing, is the use of text messages to get the attention of the User, to a fake website or a Phone number in order to obtain information about the particular user. These messages seem to have been sent by real institutions like banks or any other other real companies with services on the internet ,and may compel the recipients to update his/her account information or address some so called 'security issues' [11]. For this reason, smishing has recently become used frequently, since attackers understand that people trust in the smartphone a lot. In principle, and as in the case of vishing, smishing leverages the use of fear or something important so that the victim responds impulsively and not through proper analysis of the received message.

Angler Phishing: Angler phishing is an emerging and complex type of phishing that occurs in social media network. In these attacks, the attackers mimic authentic customer care services or genuine channels, could be Twitter, Facebook, Instagram Account. They can reply to the customer's complaint or Justification by sending them links to what look like official brand website but are actually fake phishing sites. Lanander phishing is designed to lead the user onto typing in some form of personal information or clicking on the link [12]. As much as many user prefer to stick with customer service conversations on social media platform angler phishing is indeed a good approach to social engineering in order to gather information from these users.

Clone Phishing: Clone phishing is a technique where in the attack launches an original message where the intended victim in some way has restricted the alteration capacity of the message. The attacker replaces an original attachment or link with a forged one. Knowing that the email they are receiving looks almost like the original email which the victim has received in the normal course of his work, the possibility of the victim getting trapped in the cyber-attack is way too high. Clone phishing is typically used in sequence with the first attack or whence an initial legitimate mail containing an evil attachment is already recognized [13]. It is a sort of exploitation designed to take advantage of previous message familiarity by the victim.

Man-in-the-Middle Phishing (MitM): While it can be subclasses as a distinct heistic form of phishing it is not always quite considered a form or man in the middle attacks or MitM. In these attacks, the cybercriminal sits between the target and a trusted party, such as a bank, or an online shop. The attacker may intercept the data being transfer and modify it, intercept the login names or the financial transactions and get hold of the secret details. These attacks could be over the air using phishing techniques where the owner of the data is led to a site where their data is copied before getting bytes to the right site [14]. People are becoming more pluralistic as with every new method the hackers rise to target more and more persons, programs, application and organizations. Some of the well-known types of phishing include; normal phishing, spoke phishing and whale phishing and although the attackers engage in these, they still perpetrate the crime get into secure computer networks to retrieve and pass on large quantities of private information. The varied kinds of phishing threats ought to be identified as well as different methods of preventing them, explaining the importance of protection against and combating cybercriminal activities using technological platforms computational solutions and keeping in mind about the computational system users.

BULLET: Jurnal Multidisiplin Ilmu
Volume 3, No. 05, Oktober-November (2024)
ISSN 2829-2049 (media online)
Hal 696-712

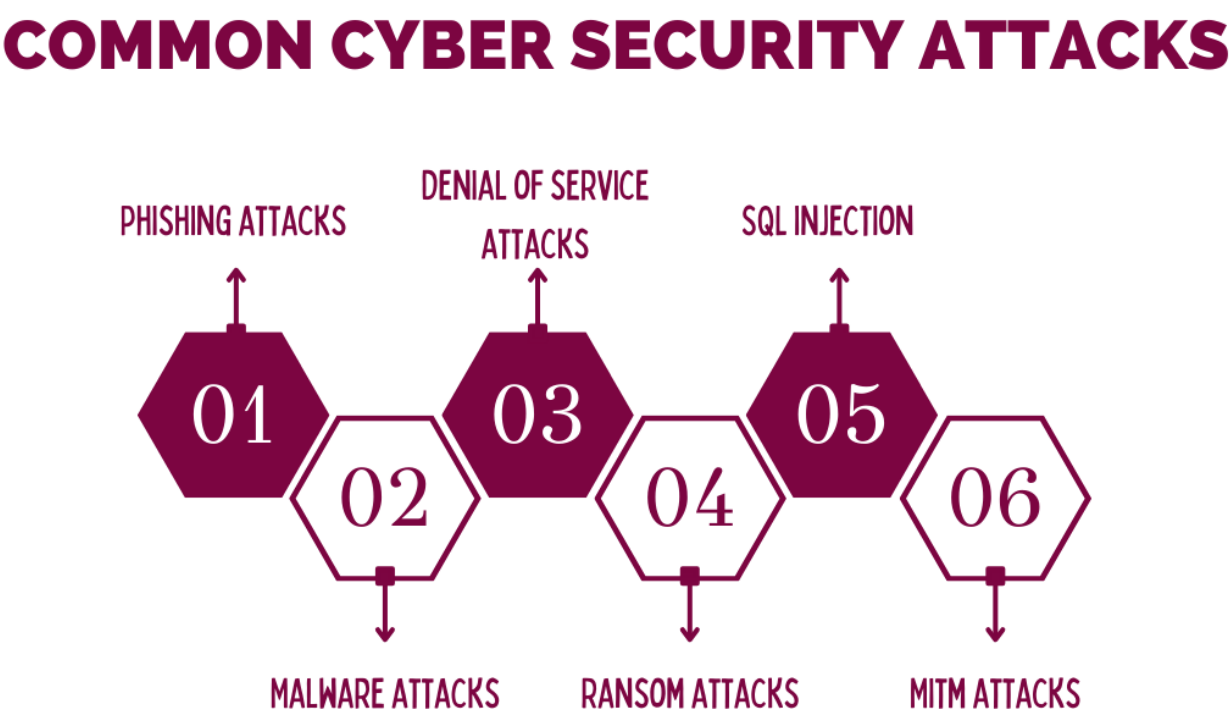

Figure: 1showing common cybersecurity attacks

TOOLS DESIGNED FOR THE PHISHING

Phishing is also based on psychological and, in particular, trust characteristics and can use elements in technical attacks that are intended to lead the victim to perform adverse actions. About Hacker and his work: There are many schemes to increase the effectiveness of the attack and start with the simplest Social Engineering and end with the most complex stages models. The case situation therefore enables one to come up with various angles that offenders employ in phishing as well as steps to be taken in order to deal with such probes. In this segment the author captures some of the simple and most common techniques employed in phishing attacks [15].

However, majority of the phishing attacks are based on social engineering, where the attacker wants people to surrender their carefully guarded secrets, or to do something that will be in the best interest of the attacker. Phishing attack which is the main strategy employed by the attackers mainly relies on the trust, emotional or, fear of the victim. There are two usual tricks used by the attackers in the message: The first one of them gives the feeling that one is at the mercy of the other – for instance Your account is under threat, click here to protect yourself In the second one, the feeling of loss is employed – for example This is your lucky chance to get something big, but it will only happen if you act right now [16]. It puts pressure on the victim to move immediately without thinking twice about much of the premises that it established. They also escalate the level of credulity since burglars can 'seem' to be belonging or affiliated with the same company, a companion or a well-established organization. Such approaches to attacks make phishing very effective particularly if it is combined with other kind of frauds.

Spoofing can be deemed as the action both in the imitation of communication – such as Email addresses and phone numbers or Web sites in the attempt to make it look as if an attack is a genuine one. The details used in email phishing scams also include defeating the purpose of the sender's address to show that it came from the sender's bank or company, or a close friend/associate. Examples of these include logos, signatures and such other names or phrases which everyone readily associates with the authentic entity in question. In addition to email spoofing, phishers may also spoof web URLs, creating web sites that are very similar to genuine famous organizations? The purpose of most of these sites is to get the user to enter in their login info, personal information, or payment information. This means, users do not know that they are on a phishing page since it has the look alike of the original website [17].

Unfortunately, being scammers, gullers may have web addresses, which actually are a copy of the real web-address, but when one types it, the page will show that you are in the real web site. It appears very similar to real organizations URL strings but there are extra letters and characters at first glance. For example, a phishing URL replaces one of the characters of the official Web site of a bank with a similar looking character, for example faceb00k.com instead of www.facebook.com. When conducting phishing for example through e-mails or even through messaging services, the attackers leave these links to these websites and encourage the user to click on them in order to fix or update their accounts [18]. The user is taken to a fake site once they have clicked on the provided link and the actual services credentials are then harvested. This scheme consists of evolving a very similar name to that of a genuine site; or a name very similar to a true site's name. These are actual representations of firms and organizations that they imitate and other are liberal misspellings of the real domain name of websites. For instance, while the regular likely URL may be 'www.amazon.com', the phisher is likely to use 'www.amzon.com'.

As the same as the above, typo squatting is another that works on people's typo mistakes, which users make occasionally. Second, unsuspecting users frequently mistype the URLs and likelihood is high for the attacker to capture a correct misspelling of the actual URL, hence making a good domain-phishing site. The other advanced technique employed in phishing activities is sending of virus infected emails to the targeted individual. This is mostly true when a victim opens an email attachment or even just clicks on a link in a phishing email. Through the email the victim is compelled to interact with the string of text, if the string of text downloads and or installs the malware the device is infected, or the string of text executes other process in the operating system causing the virus to spread. Phishing emails may lead to websites and emails that look genuine, with a link to websites that harbors download malware or have attachments with an invoice, document, or image with malware. For instance, when a person downloads an attachment on an email message the might trigger the ransom ware, spyware or the trojan horse that enables the perpetrator to gain control of the target computer or pirate the information [19].

Misuse of credentials is one of the most visible goals of specific phishing attack methods. Here the phishers employ fake login form or any other fake site similar to real internet site aiming at extracting UIDs and passwords from the global users of the Internet. They may be contained in the URLs of the bogus Web sites employed by the phishing assaults or in the link given in the body of the phishing e-mail or MMS. To the victim, it is made to understand that they are entering their data in a real website for instance a banking area or in a social site. Subsequently, the attacker inserts the victim's credentials and then he or she controls the accounts and information input for identity theft or fraud and other malice purpose [20]. Such credential harvesting methods works well if the phishing website looks like the original one with logos, colors and layout.

Common techniques often tricks opens a new what seems to be ferent file format such as PDFs, Word, Excel and etc as email attachments. By the way, these files can contain macro, script, or some sort of deliberately inserted virus to infect the computer with malware if opened. These attackers might give these files a name which will make the victim open it for instance invoice, receipt, job offer, etc, For example, the email might state they wanted the recipient to review an invoice which was included in the body of the email. If the victim opens the file, then several programs run on the device and the system may get into viruses or ransom ware. Although it cannot be actually classified strictly as a kind of phishing attacks, the man in the middle (MitM) attack can be started with the help of it. In these attacks, the cyber attackers intercept and modify the messages between a target and a normal service they wish to communicate with, say an online banking session [21]. This is because, most of the time, the phisher develops an exact replica of the website they wish to lure the victim into, which has a login page that once the unsuspecting victim fills with his authenticate details the page will forward the victim to the original site while the attacker records the details entered by the victim.

Another form of MitM attack can be most successful especially in the case of controlling the Wi-Fi networks or utilization of Trojan ordinations to capture the technique of data transmission, makes the practise of phishing most secret or ineffective to be detected. Phishing attacks can be staged using a variety of methods, and the methods, by which they are staged, can be expected to be as constantly shifting. The first ones are as simple as social engineering and spoofing, relatively crude and unsophisticated as compared to others such as the malware payload, man-in-the middle attack etc [22].,iyorum phishers employ psychological and technical warfare. Such techniques may well be very useful in so far as they go and that is if they are based on trust, time constraints, or lack of knowledge. Since the type of phishing attacks has changed, various measures toward increasing security and sensitivity should be made besides making users aware of phishing threats.

BULLET: Jurnal Multidisiplin Ilmu
Volume 3, No. 05, Oktober-November (2024)
ISSN 2829-2049 (media online)
Hal 696-712

SOCIETAL IMPACT OF PHISHING TO ORGANIZATION AND INDIVIDUAL

For just a single person, the ramifications could be lethal encompassing the financial damage, insult to clientele/shareholders/employer's integrity, permanent compromise of an institution. Although the effects of the phishing attack may not seem so mortar, shakes can be many and serious. Phishing attacks: This part of the paper seeks to explain the various effects of phishing attacks and the effects that come with them to personal and organizational users [23]. To people and organizations alike, one of the ways of realization of a phishing attack is the aspect of money loss. Consequently, a person becomes a phishing scam victim, and may disclose credit card data, account numbers or login credentials to the attackers, thereby experiencing unauthorized operations or identity theft. This results in much loss of cash as giant is seen leaving the victims struggling to know how they are going to get their cash back.

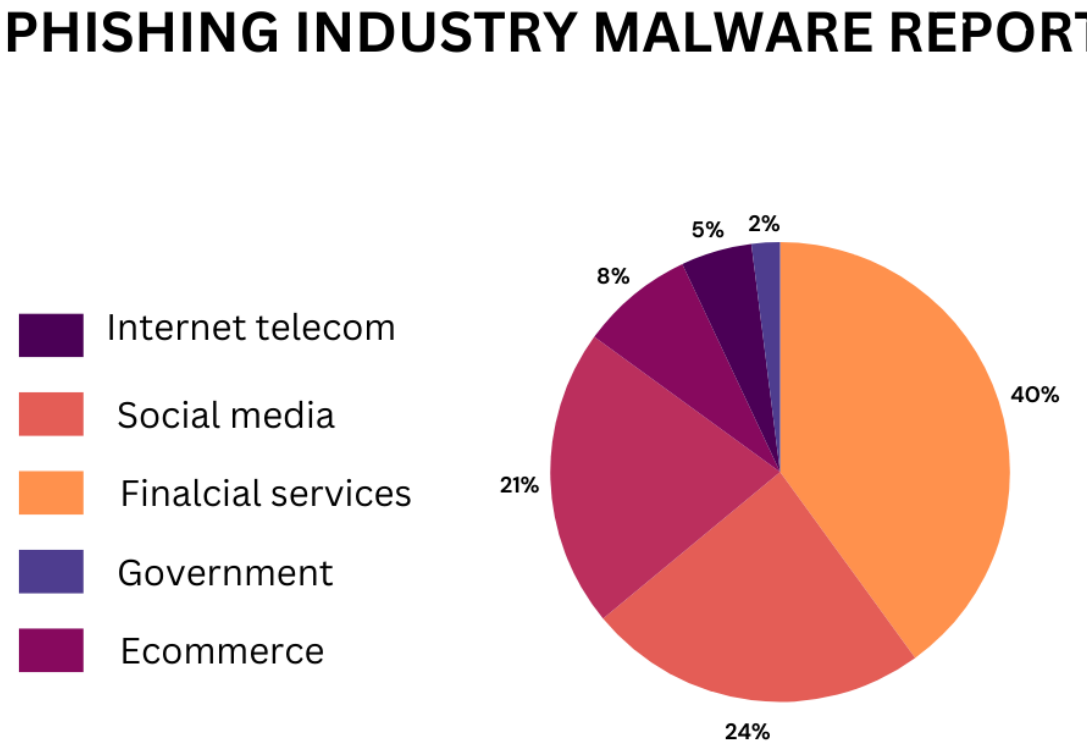

Figure: 2 showing phishing industry malware report

As for what happens in case of the phishing attack, the losses are usually higher when it comes to organizations. This could be petty cash which has been chucked through direct fraud like moving of cash through wired operations or indirect cost that may include cost of evaluating the losses, making required adjustments and refunding clients who may have been affected. Sometimes phishers can use the phishing as interim to other more advanced scams such as the expiry of ransom ware which calls for a lots of cash for the unlocking of important data. The other effect of phishing attack is reputational loss this loss is felt even more when it happens to an organization or a company. While phishing is considered a moderate malevolent act, it is highly dangerous for an organization's reputation if an attacker manages to phish an organization's information, organizational data or customer's data [24]. Consumer trust results from customers' belief that their information will not be used or shared by businesses that do not handle such an obligation lead to business loss, significant public relations disaster and consumers distrust.

For instance, customers may decide to get the services from other organization because they are aware that their data has been passed on to hackers who conduct phishing attack or worse cases one may write bad reviews about the organizations service or products, or even sue the organization. In some industries especially where an organization is expected to protect data and privacy of people this brings legal repercussions and company losses because of failure to uphold the laws on protection of data. Phishing is usually used in online fraud and is a gateway to other kinds of attacks including data theft where the attacker gains access to information of customers, the organization and even other people. Phishing could work if the receiver clicks on a given link provided or opens an attachment which in fact holds malware or some kind of spyware. It can then grab data and this makes it easy for attackers to infiltrate a company or to steal a given individual's data [25].

Where it involves the people, data breaches can lead to loss of identity or credit card fraud or invasion of body privacy. For organizations, the things that can be stolen include customers data, ideas or any data that an organization might consider sensitive can be sold in the dark web or used to blackmail an organization making a breach more severe. Whenever legally implicated entities that are involved in data dissemination are subjected to phishing attacks, and they do not have sound procedures for protecting sensitive information, they will be in breach of the regulations. The GDPR and the CCPA as well as other specific laws require that merchants to ensure personal information is protected. The loss of customer data due to a phishing attack can trigger investigations, fines and lawsuits [26]. Sometimes organizations become legally liable for not sufficiently guarding information or for insufficient or delayed notification of clients, customers, shareholders or employees. For instance, the GDPR permits processing of data of the individuals without their consent if it is in their best interest, which is often the case with children's data, and very soon organizations will be expected to notify the affected individuals of data breaches within 72 hours of the organization identifying the breach. Any non–compliance to any such regulation may lead to fines and erosion of long-term market reputation in the organization.

Most of the phishing leads to operation interferences and it becomes worse when a malware or ransom ware is added on the phishing con. For example, ransom were will actually threaten organizations and lock down key systems and information for retrieval unless a particular sum is paid. Such attacks can interrupt tasks already in progress which are common in a business and result in massive waste of time [27]. In addition to ransom ware attack, phishing attacks can install other applications that affect the performance of the system or cause software to freeze or crash; and other ways through which an unauthorized person can gain access to network systems. To organizations, they lose sales, the time they spend investigating the breach and the time spent to rectify the issue is costly. Most of the time these interferences emerge as the business is in the process of providing services or products meaning that the business loses clients and sales. Phishing commonly occur in the initial phase of cyber-attack and even can occur in the subsequent phases too. Even more frequently once a cybercriminal has compromised an individual or an organization and managed to get in using a phishing attack, it sets up more tools for reuse, including a key logger, a backdoor, or any kind of spyware. Such an open door can allow the attackers to continue monitoring activity, or pry into more information, or continue with numerous attacks at other times [28].

In businesses, these chronic weaknesses can lead to a much greater security compromise because after the phishing attack the attacker would be able to use the initial entry point through which he or she got into the organization's network to gain access to other parts of the network. While these vulnerabilities remain invisible for a long time, they pose the increased threat of longer actual breaches of critical infrastructure targets. Thus, for organizations, a successful phishing attack also weakens its trust with the organization's workforce and their morale [29]. Employees of the organization feel that they have lost their private information or else the organizations' confidential commercial information becomes available to the public due to a phishing attack. Also, the 'internal trust' in the organization's security measures decreases, and, therefore, the productivity: the public cannot believe that in their own company data is safe and sound. They may resist sharing information thinking again they will be fired which will influence how things are done at the workplace. (Vertex 7) employees will be even more skeptical to other Outside-in communication such as email or short message service, the efficiency of which will diminish regarding the delivery of critical business messages.

Phishing attacks in general, and their short term and long term impacts on the individual or organization. Firstly, there are financial risks, a company can be financially drained, and litigation can be very disastrous where privacy is compromised, or operations are interfered with. Organizations must implement good defensive measures in order to avoid getting attacked via phishing for instance, organizations should warn employees on the dangers of phishing scams, the organization should have good secure network policies, and most importantly have a good backup system in case they have been attacked. In the case of users personal knowledge that how these phishing attacks works and practicing secure internet usage is very importance to prevent oneself being victim of such attack

[30]. The presentations of the concepts introduced will help the individual and organizations to adequately defend their data and property against phishing threats after pointing out the implications.

PHISHING ATTACKS CAN BE PREVENTED

Phishing risks pose significant threats to both occasional users of an internet connection as well as business entities and it is important to point out here that risks can be avoided through use of technological interventions, awareness and preventive measures. This section will focus on outlining the measures of how to guard against phishing and more specifically; prevention strategies, ways of identifying phishing and handling the threat. The best way of protection against phishing is through launching programs that seek to raise public awareness [31]. Since the phishing attacks are more depending on the social engineering that aims at targeting the users they need the audience to be aware of the tricks used in the phishing so that they can avoid complying with them.

Recognizing Suspicious Emails: Citizens should teach on how to screen the mails for any chances of phishing; any incorrect spelling within the domain name, any unknown sender address, any themes like a push to step up before it is too late, any attachments or links do not seem right. They also should be advised to check the receipt notices of sensitive information by replying to the supposed sender [32].

Training on Phishing Simulations: The best example lies in where organization conduct phishing simulation where the employees are given fake phishing e-mails. These drills help the employees to be more knowledgeable on various phishing attempts common in the workplace outlook.

Ongoing Awareness Campaigns: When conducting security awareness it should not be a onetime affair. Various exercises, circulars, and advertising will continuously reinforce the message to be more conscious on the Internet. A beautiful example is when the attackers get the username and password of a user through a phishing exercise; it will be difficult to go further because of MFA. MFA on the other hand involves users providing more than one factor to be verified in order to gain access to an account; the factor involved would be a knowledge factor, possession factor and an inherence factor. Because more than one factor of identity is needed for the MFA, even if the attackers have the passwords put in front of them, the MFA makes it considerably tougher for the attacker to succeed [33]. At present, virtually everyone uses the method of two-factor authentication for accessing key applications or performing financial operations – that is why phishing initiatives generate fewer results.

Anti-phishing Tools and Email filtering

It is therefore wise that organizations adopt high end email filters for detection as well as outright blocking of the phishing emails even before they get into the inbox folder. Modern email security solutions incorporate various techniques such as:

Spam Filters: All of these filters are used in filtering messages like spam and could in fact include actually phishing emails. Now, they use algorithms to scan through emails for another set of features used by the attackers during phishing [34].

Content Analysis: Most filters are capable of reading the entire content of an email including any link, attachment or any other word in the email that may be a phishing link.

Domain-Based Message Authentication (DMARC): SPF and DMARC together with DKIM help in the initialization of emails with reference to the received emails so that emails that tend to use fake email address do not pass through [35].

Machine Learning and AI: There is then more complicated forms of machine learning or artificial intelligence that continue to analyze the traffic of emails for new forms of phishing, the higher skills towards detecting new phenomena hence being made possible.

General Site and Link Restricted Features

Probably the best way to keep users on guard about where they click and which websites they proceed to is effective enough to ward off most phishing attacks. Some techniques to reduce the risk include:

URL Validation: It can be useful to advise users to ‘mouseover’ before they click in order to check whether the link goes through to a genuine site or a phishing page. Users should avoid the domain name of the website that has been spelled in wrong way or slightly different from official name [36].

Browser Safety Features: Most of the current web browsers main versions come with added security bars, which warn users when they try to connect to a bad or phishing site. These features can deny connection to any undesirable address, thus shield the user from being prey to the phishing scams.

HTTPS: To ensure the websites are safe, it is recommended that an organization uses the HTTPS (HyperText Transfer Protocol Secure). People should type valuable information only on the sites with a padlock in the status bar and 'HTTPS' nearby [37].

Incident response and Reporting Procedures

Nonetheless, there may always be a case where some of these phishing attacks would still make their way through to the targeted community. Where such situations occur, it is a proper practice to ensure that the incident response procedures are clearly spelled out. This plan should include:

Quick Detection and Reporting: Respectfully, employees and users should be made to report any messages or activities that they consider suspicious to the organisation's IT/Security department on sight. It enables the organization to respond quickly reducing the probability of further compromise happening.

Containment and Remediation: If an organization has fallen victim to a phishing attack, then on the realization of the fact it has to act fast to mitigate the breach. This may involve isolated of the system or part of systems, change of passwords, cleaning of virus or worm, and informing users or customer as appropriate [38].

Root Cause Analysis: There should always be an examination of a given attack in its aftermath, especially to determine how a given attack took place in the first place as well as to point out vulnerabilities in the organization's security systems against phishing attacks.

New Gen Security Technologies

Organizations also can use more developed security technologies in preventing successful phishing. Some of these technologies include:

Endpoint Protection: Ongoing anti-virus and anti-malware software running on all units are useful in identifying and preventing mostly all files and documents sent through phishing including fake course information. Endpoint protection tools can also scan devices for signs of malicious activity and it can also prevent known phishy sites [39].

Behavioral Analytics: This is why the behavioral analytics tools track user behavior and are, for instance, able to identify that the user performs the logging in at suspicious hours or performs the large data transfers, or accesses sensitive information [40].

Threat Intelligence Feeds: Security teams can therefore get feeds which will give timely information on new phishing campaign. It shows that, by being aware of the newer form of phishing and its modus operandi, organizations can be more ready and able to deal with such attack.

Regular Security Audits

It is, therefore, crucial for an organization to conduct security audit and/or vulnerability scan periodically. These audits should include:

Phishing Simulations: This type of approach of using fake fake phishing emails to employees and company systems routinely assists in identifying lapses in compliance with anti-phishing training and response procedures [41].

Vulnerability Scanning: An ongoing vulnerability scan of all internal and external aspects for potential flaws like unaudited applications or unsecure settings can minimize chances of phishing being …

BULLET: Jurnal Multidisiplin Ilmu
Volume 3, No. 05, Oktober-November (2024)
ISSN 2829-2049 (media online)
Hal 696-712

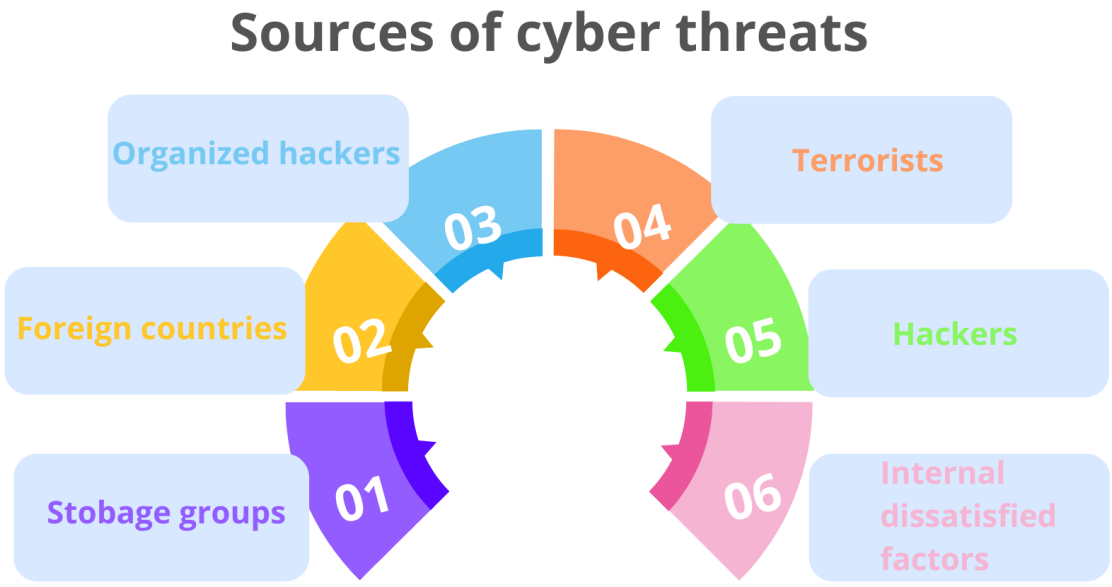

Figure: 3 showing sources of cyber threats

Penetration Testing: Penetration testing is a good way of testing the security systems since the teams doing the testing know the loopholes as no other attacker does. Phishing emails can be a part of this testing process, usually using imitation or copied phishing attacks. Preventing the latter depends on the in-depth protection of sensitive information and using various technologies that analyze attempts at phishing, as well as a strong educational campaign and quick response systems [42]. This paper also shows that user awareness training on new emerging threats, use of multi-factor authentication, advanced email filtering techniques, and good incident response measures, can significantly reduce the susceptibility to phishing. This means no defense system is perfect but getting more proactive and putting up multiple layers of protection against data breaches is the only way to prevent multiple attacks such as the one that is as subtle as phishing.

NEW WAVE IN PHISHING ACTIVITIES

Phishing scheme is still relevant and very active because the hackers never stop with their innovations. In turn, as the methods and means used by the attackers are becoming more and more perfected, the problem of becoming a victim of a phishing attack becomes more nuanced and systemic. Knowledge of these trends can prove invaluable to anyone that would like to better understand what is out there in the world of cybersecurity, as well as strengthen and adapt his or her own protection strategies. In the following part, the author describes some of the recently observed trends in phishing attacks, discusses which types of attacks have become popular and what new paradigm shift they bring [43]. While phishing provides attack a general attack that is implemented on diverse people, spear phishing is a specific type of phishing where attackers aim at particular people or corporation. These attacks are very often based on personal or professional profiles of the target that is researched in advance.

For instance, a scammer may use the details from a fake social media account, a target's corporate site, or public domain records to make a message or an email look legitimate. Spear phishing is usually aimed at top management and key employees, other IT workers interested in company data (a type of attack called 'whaling'), and company accounts. Spear phishing has a greater chance of success because of the level of personalization – which is why it is such a danger. This new type of phishing specifically targeting organizations has been christened Business Email Compromise (BEC). With BEC attacks, the criminals pretend to be the company's top officials or business partners to demand wire transfer or payment. These attacks typically have a theme of business e-mail compromise, through which the attackers take over legitimate e-mail domains to prompt transactions [44].

BEC attacks are based on deceiving relationship in the company and often are very complex. Often the attackers study the organization and the flow of its financial transactions before the phishing emails are sent out. BEC attacks have financial losses and particularly large amounts of money that take time to detect because they are not

immediately noticeable. Increasingly, social network and Messengers became a virile base for phishing as such platforms become more popular [45]. It is a form of phishing where the bad guy pretends to be a friend or some other person with a social networking site such as Facebook, twitter, linkdin, etc and get person to give his or her details or clicking a link.

Some phishers may also use the users' messaging apps including WhatsApp or Telegram or even through an SMS (smishing). Such attacks are more covert in that they exploit the legitimacy of personal communication. The attackers disguise themselves as friends, family members and other entities or companies, which the victim knows and can trust him or her, in order for the victim to click on the links and send information, or download attachment files. As voice communication technologies became more popular, vishing – or voice phishing – became another way to take advantage of trust. Normally in vishing attacks, phone calls and voice messages are made by an attacker to mimic the identity of a trustworthy friend or an organization such as a bank, government office or a technical support group. The attacker may come up with all sorts of reasons, for example, he will state that he is a team investigating fraudulent activities or ask for credit card details, account details, or social security numbers [46].

Vishing can be especially effective because the authorized, urgent tone of voice communication is mobilised. The authors identified that offenders are inclined to create a context that demands the respondent to provide certain information in one way or another; otherwise, fear or time pressure contributes to the attackers' success. More recent innovations in the use of tools include artificial intelligence and deep fake technology which cybercriminals use in improving on their work in the use of phishes [47]. Synthetic media, the use of realistic fake audio and video, is also being used in advanced phishing attacks in which people are conned into thinking they are talking to a co-worker, employer or spouse.

For instance, the attacker may use deep fake voice called voice convincer, where the attackers mimic the CEO on-phone-call and directs the employees to release some cash or give sensitive details. These are complex attacks and those are highly realistic attacks thus making them near impossible to identify and to prevent. Therefore, as deep fake technology increases, it greatly difficult for cybersecurity professionals to differentiate between real and fake messages. Although not a recent type of attack, credential stuffing is gradually being associated with phishing schemes. Credential stuffing is a form of brute force attack where the attacker uses username and password pulled from previous security breaches to try and log into another website or application [48].

Credential stuffing is most commonly married to phishing where the attacker uses it to obtain usernames and passwords or direct users to fake login pages. If attackers have obtained the login details via phishing or data breaches, then they use botnets to try to log in a service. When users receive phishing emails, the attackers add credential stuffing into the mix to raise the likelihood of getting into more accounts, as many users tend to reuse passwords across their accounts. Even QR codes which can be considered as a relatively safe and fast method to share information is an object of the emerging type of phishing attacks [49]. Cybercriminals can embed dangerous QR codes randomly anywhere, on walls, in products, or use them in advertisements. These QR codes can when scanned lead the victims to phishing sites, install malware or take them to fake payment sites.

QR codes most of the time do not show the actual URL or content before they are decoded and hence offer the attackers a unique opportunity to entice users to visit malicious sites without fully realizing it. Users should fully understand this and be careful in using QR code scanning tools especially that check the URL legitimacy before granting access. Since the popularity of the use of mobile devices rises higher and higher, most of the phishing scams now are aimed at smartphones and tablets. Similar to mobile phishing, smishing occurring through SMS text messages exploits small screen space and the user's predisposition to click links or download an app. This is as Trojan attacks can involve sending of SMS messages which appear to have been sent by the actual sender, be it a bank, service provider or government agency where by the user is redirected to a fake login page or even enticed to download an application [50].

Mobile phishing also refers to the use of what looks like forged applications that would be expected to originate from reliable organizations. After the installation, such apps may also steal data, message the user's contacts, or even text them with phishing links, or even redirect the user to fake phishing websites. This is perhaps because cloud is now the most prevalent tool and service used in various organizations and continues to grow, this has made attackers focus on cloud platforms with the intention of conducting phishing [51]. For instance, phishing attacks can be executed a fake link to Google drive, one drive or dropbox for file sharing. Some of the most common examples are phishing emails from the organization's verified personnel or from other colleagues or partners with whom the recipient has formerly worked with, where the links take the victims to fake documentation.

Further, some of the phishing typology includes cloud service account phishing, where the intruders employ the cloud provider's communication channels to deliver the phishing messages to other users within the same

workplace, which tends to be more believable and risky. Phishing is still prevalent to the meaner because hackers follow the latest trends and technologies in the society. While once attackers were content with spear phishing and business email compromise, today, we have deep fakes and QR code phishing. The use of mobile and cloud in addition to using voice as a means of performing the act of phishing is a new inflection point to the threats hence the importance of offering information to the consumers/clients. To counter these emerging phishing strategies, the necessary tenet is vigilance, layered with levers in security, and the recognition that every day brings new threats the networks must combat. In portraying new patterns likely to be adopted in the arty of phishing, everyone is safeguarded with new ways that can be used to reduce risks and maintain security of data [52].

DEFENDING AGAINST PHISHING: BEST PRACTICES AND SOLUTIONS

Since phishing attacks are becoming more and more sophisticated, protection against the type of threat is not limited to one or two tools. Users and institutions need to work out a set of technical measures, inform users, and apply strict precautionary measures in order to minimize the threats and consequences of the phishing popularity. This section includes ideas and approaches and showcases the practical ways of protection from phishing attacks and stresses that the threats are dynamic and the protection measures require constant update. Several motivations have been taken into considering the security problems so that users should be protected through training: the best countermeasure against phishing is user awareness of the threats and techniques used by the attackers [53]. This is following the fact that phishing mostly involves tricks and manipulation, therefore increasing the level of awareness can greatly help those at the receiving end avoid such scams.

Phishing Simulations: Phishing simulation exercises on the user's side is effective in helping the organization's users to identify phishing scams and how they should respond to them. These simulations can capture many real life situations, and these can effectively be used to train the employees to detect a number of signals that should alert them to some risk situations.

Regular Training: The management needs to provide cybersecurity training frequently because employees are subjected to phishing campaigns constantly. 'autres points de formation devraient concerner la manière de détecter les e-mails phishing, en évitant les ouverts et les pièces jointes suspectes et en informant les specialized threats [54].

Promote a Skeptical Mindset: Promoting critical approach when reading the received messages as well as when dealing with the messages containing the request to provide personal data or create the sense of the urgency can also let users avoid phishing. Training should point out to it is critical when there are unusual requests made and seek to get a clearance first. There are few technical defense mechanisms that are effective against phishing and multi factor authentication is one of them. In fact, MFA introduces an extra protection factor compared to common passwords, often making it quite difficult for the attackers even if they compromise the username/passwords through phishing [55].

Types of MFA: That is why the acronym MFA can mean what the user knows, such as password; what the user has such as a smartphone application or token; or even what the user is, in terms of biometric authentication. Such forms are quite standard: a simple one-time password sent in an SMS message, an application, such as Google Authenticator or Windows Authenticator, or a fingerprint or face scan [56].

MFA Everywhere: All accounts and services should be protected by MFA, and then anyone who uses email, the cloud service, or any utilities that involve transactions of any kind have to use MFA. MFA highly reduces the probability of phishing as for instance the attacker has to find his or her way through at least two factors. Since, as we have seen, phishers predominantly use email as the delivery media for their messages, robust and efficient email filtering is required to counter and preempt phishers with effective filtering of phishing messages. These turn key solutions depend on signature based detection, machine learning and behavior analysis for detecting the messages [57].

Spam and Phishing Detection: The applied technologies of email filtering enable the key potential threat, such as the meaning of the received message, the files, links, and metadata of the sender. These systems also can be created using machine learning that makes them increase the effectiveness of subsequent phishing campaigns [58].

SPF: Of course, SPF checks that the email is coming from the allowed server to the specific domain. For instance, it checks that a specific sender's IP address is in the Domain Master list that is in the DNS of the Domain.

DKIM: With DKIM, there is authentication of whether the message has been altered in transit, and the sender's domain name is genuine.

DMARC: DMARC actually builds on SPF and DKIM, and the 'policy' which should be enforced if a message is not signed according to SPF and/or DKIM. It allows the domain owner to set how the system should treat a spam message or whether to delete or block them [59]. Such protocols also help in reducing email spoofing that can easily allow the attackers to represent as genuine some organizations and forward an email that is full of phishing. It is about and Endpoint Protection that have major roles when it comes to protection against Phishing Attacks. Critically significant in protecting the endpoints where phishing attacks take place is that cybercriminals always use such a strategy to introduce malware and obtain unlawful entry into a system.

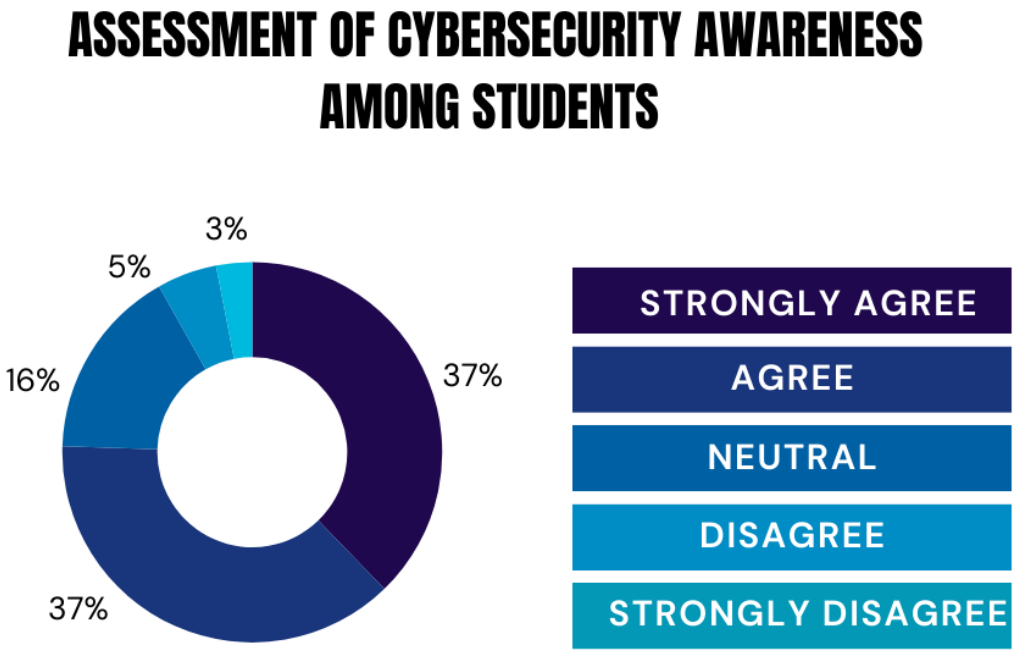

Figure: 4 showing assessment of cybersecurity

Antivirus and Anti-malware Software: Having the latest versions of endpoint security software can reduce the introduction of the new threatening payloads into an organization's environment as contain the phishing emails, ransom ware, spy ware, key loggers etc [60].

Endpoint Detection and Response (EDR): EDR solutions enables the continuous monitoring of the endpoint activity and the ability to detect a possible phishing happened or the subsequent infection of malware. Such systems are needed for filters in the event of threat identification so that the level of damage can be regulated. That is why the Zero Trust approach is gradually gaining popularity as an approach for combating phishing. Specifically in Zero Trust schema there does not exist an implicit trust policy for everything both internal and external [61]. What is more, each of the access requests is checked as frequently as possible before one is granted entry.

Micro-Segmentation: Concerning the notions of Zero Trust, it is assumed that networks are segmented at the micro-level, as well as the economic motion of the attacker within the network environment. While the specific area that is being targeted in a phishing attack is compromised, others areas of weakness are prevented from being exploited to the maximum [62].

Continuous Verification: Unlike Zero Trust, the credential validation is not a one-time process; that is, the user and device remain monitored for mal activity and thus prevent an unauthorized actor from launching a phishing attack and attaining prolonged access to the high-risk systems. While studying the flow and exchanges of information between the organizations and across industries, I also noticed that inter organization information sharing is also pointed as a new vital part in combating the menace of phishing. By sharing information and sharing intelligence various organizations are well poised to identify these newly emerging phishing attack in the market [63].

Threat Intelligence Feeds: There is the use of real-time threat intelligence feed to update an organization on existing common threats such as phishing threats that relate to available IP address, URLs and email signature of

the phishing campaigns. This one can be used to update the filters one has for e-mail, bar blocking those certain IP addresses that attackers use frequently among other things.

Software Patching: PORT/PROTOC OL1: That may seem like a no-brainer, but this is a great way to lessen the effectiveness of phishing scams that involve existing threats and also to make certain that the applications they are using and the clients and servers they are connecting to are also updated. Patch management is one of those corporate security procedures which should be done periodically and as frequently as necessary [64]. The strategies that can be used to avoid falling victim to the attack entail the following skills and technological equipment's. In the prevention of phishing attacks, measures need to be put in place one of them being organizations and people to employ the following; best email filtering, Multi-factor authentication, advanced endpoint security, and lastly people should be sensitive to the tricks used by phishing attackers. Now that the phishing practices have become very sophisticated, the protection must employ such sophisticated systems as the machine learning, the zero trust model and live threat feeds. And the final protection line is a multilayer defense line and the trained personnel in the fight against phishing and in the modern world.

CONCLUSION

This is gets threatened by phishing attacks as the most prevalent, and the most unchanging form of attacks that the cyber criminals they do not alter their strategies. From this review we find out some of the trends followed by the attackers, the strong weapons used by the attackers, and the fundamental precaution, approaches, and new technologies required to fight against such threats. Phishing is still a security issue since people are the weakest point; therefore, the user's awareness needs to be repeated regularly to reduce the efficiency of phishing attacks. That is why, the users' awareness, as well as strengthening a critical approach towards the received e-mail, in addition to protection measures such as MFA can contribute greatly to the decrease of the threats of phishing in an organization. Moreover, through inbox controls and best heuristic together with machine learning with a bang, then a basic level protection from phishing emails is acquired; quite secure email authentication measures such as SPF, DKIM, and DMARC do cut out this type of malicious email from reaching the users.

As the level of phishing advances with time especially in the neaer future, use of various AI techniques such as artificial intelligence, machine learning as well as the behavioral biometrics tools will be very useful in countering this type of threat. The same tool in the hand of the attacker helps make the emails appear genuine while on the other side the same tool helps a defender identify and recognize chances of irregularities and or threats. Moreover, new. Coming cyber criminals have started using Phishing-as-a-Service (Phaas) which makes it very easy for attackers to conduct campaigns at a larger scale, thus, further stressing the need for organizations to beef up themselves against such ever dynamic threats. The chances of impact from successful cyber-attack can be minimized because none or all the entities are universally trusted and every single request for access is checked by adopting or practicing the zero-trust security approach and report the users' behaviors. Endpoint protection, most organizations' frequent security audit, threat intelligence collecting and practices inside companies, gave extra layers to organizations against phishing campaigns and emphasized the importance of cybersecurity.

The future advancement for protection against phishing will be cooperation engulfs in the industry such as block chain technologies for secure e-mail and digital identity. When organizations have a robust proactive and resilience cybersecurity organizational culture, it becomes feasible for the organization to mitigate incidences of successful phishing attacks and reduce the enduring impacts of the attacks, if any. Thus, anti-phishing is a multifaceted problem that involves knowledge education, security tools and technology and organizational commitment. By these cooperation and synergy, Personal and Business entities are equally placed to protect themselves from one of the leading Cyber threats today and this make the future safer.

REFERENCES

1. Jangjou M, Sohrabi MK. A comprehensive survey on security challenges in different network layers in cloud computing. Arch Comput Methods Eng. 2022; 29(6): 3587–3608.
2. Alam A. Cloud-Based E-learning: Scaffolding the Environment for Adaptive E-learning Ecosystem Based on Cloud Computing Infrastructure. In Computer Communication, Networking and IoT: Proceedings of 5th ICICC 2021. 2022; 2: 1–9. Singapore: Springer Nature Singapore.
3. Seifert M, Kuehnel S, Sackmann S. Hybrid Clouds Arising from Software as a Service Adoption: Challenges, Solutions, and Future Research Directions. ACM Comput Surv. 2023; 55(11): 1–35.
4. Nadeem F. Evaluating asnd Ranking Cloud IaaS, PaaS and SaaS Models Based on Functional and Non-Functional Key Performance Indicators. IEEE Access. 2022; 10: 63245–63257.

5. Parast FK, Sindhav C, Nikam S, Yekta HI, Kent KB, Hakak S. Cloud computing security: A survey of service-based models. Comput Secur. 2022; 114: 102580. International Journal of Wireless Security and Networks Volume 1, Issue 2 © STM Journals 2023. All Rights Reserved 25
6. Nadeem M, Arshad A, Riaz S, Wajiha Zahra S, Band S, Mosavi A. Two layer symmetric cryptography algorithm for protecting data from attacks. Comput Mater Contin. 2022; 74(2): 2625–2640.
7. Mohammed CM, Zeebaree SR. Sufficient comparison among cloud computing services: IaaS, PaaS, and SaaS: A review. Int J Sci Bus. 2021; 5(2): 17–30.
8. Ali M, Jung LT, Sodhro AH, Laghari AA, Belhaouari SB, Gillani Z. A Confidentiality-based data Classification-as-a-Service (C2aaS) for cloud security. Alex Eng J. 2023; 64(2): 749–760. 12. Butt UA, Amin R, Mehmood M, Aldabbas H, Alharbi MT, Albaqami N. Cloud Security Threats and Solutions: A Survey. Wirel Pers Commun. 2023; 128(1): 387–413.
9. Aoudni Y, Donald C, Farouk A, Sahay KB, Babu DV, Tripathi V, Dhabliya D. Cloud security based attack detection using transductive learning integrated with Hidden Markov Model. Pattern Recognit Lett. 2022; 157: 16–26
10. Nadeem M, Arshad A, Riaz S, Zahra SW, Dutta AK, Al Moteri M, Almotairi S. An Efficient Technique to Prevent Data Misuse with Matrix Cipher Encryption Algorithms. Comput Mater Contin. 2022; 74(2): 4059–4079.
11. Upadhyay D, Zaman M, Joshi R, Sampalli S. An efficient key management and multi-layered security framework for SCADA systems. IEEE Trans Netw Service Manag. 2021; 19(1): 642–660.
12. Zahra SW, Arshad A, Nadeem M, Riaz S, Dutta AK, Alzaid Z, Almotairi S, et al. Development of Security Rules and Mechanisms to Protect Data from Assaults. Appl Sci. 2022; 12(24): 12578.
13. Al-Shabi MA. A survey on symmetric and asymmetric cryptography algorithms in information security. Int J Sci Res Publ (IJSRP). 2019; 9(3): 576–589.
14. Musa A, Mahmood A. Client-side cryptography based security for cloud computing system. In 2021 Int Conf on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India. 2021; 594–600.
15. Hossain ME. Enhancing the security of caesar cipher algorithm by designing a hybrid cryptography system. Int J Comput Appl. 2021; 183(21): 55–57.
16. Akanksha D, Samreen R, Niharika GS, Shruthi A, Kiran MJ, Venkatramulu S. A hybrid cryptosystem based on modified vigenere cipher and polybius cipher. EPRA Int J Res Dev. 2022; 7(6): 113–119.
17. Sun H, Grishman R. Lexicalized dependency paths based supervised learning for relation extraction. Comput Syst Sci Eng. 2022; 43(3): 861–870.
18. Nadeem Muhammad, Arshad Ali, Riaz Saman, Zahra Syeda, Dutta Ashit, Alzaid Zaid, Alabdan Rana, Almutairi Badr, Alaybani Sultan. Hill Matrix and Radix-64 Bit Algorithm to Preserve Data Confidentiality. Comput Mater Contin. 2023; 75(2): 3065–3089. 10.32604/cmc.2023.035695
19. Kaspersky. Tips on how to protect yourself against cybercrime [Online]. Available from https://www.kaspersky.com/resource-center/threats/what-is-cybercrime
20. Exploring and analyzing Internet crimes and their behaviours. Perspectives in Science. 2016;8:540-542. Brief Study of Cybercrime on an InternetDhavalChudasama All Rights Reserved 6
21. Norton. 11 ways to help protect yourself against cybercrime [Online]. Available from https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-fromcybercrime.html
22. Kaspersky. Tips on how to protect yourself against cybercrime [Online]. Available from https:// www.kaspersky.com/resource-center/threats/what-is-cybercrime
23. HemrajSaini, Yerra Shankar Rao, et al. Cyber-Crimes and their Impacts: A Review. International Journal of Engineering Research and Applications (IJERA). 2012;2(2):202-209.
24. Helpline Law Legal Solutions Worldwide. Cyber Crimes in India-What is, Types, Web Hijacking, Cyber Stalking [Online]. Available from https://www.helplinelaw.com/employment-criminal-andlabour/CCII/cyber-crimes-in-india-what-is-types-web-hijacking-cyber-stalking.html
25. V.Karamchand Gandhi. An Overview Study on Cybercrimes in Internet. Journal of Information Engineering and Applications. 2012;2(1):1-6
26. DM Chudasama, LK Sharma, et al. A Comparative Study of Information Systems Auditing in Indian Context. Information Systems Audits for eCommerce. 2019;7(4):020-028.
27. DM Chudasama, L.K. Sharma, et al. Refine Framework of Information Systems Audits in Indian Context. International Journal of Computer Sciences and Engineering. 2019;7(5):331-345.
28. DM Chudasama, Kathan Patel, et al. Awareness of Data Privacy Breach in Society. International Journal of All Research Education and Scientific Methods (IJARESM). 2020; 8(10):303-307.

29. DM Chudasama, Darsh Patel, et al. Research on Cybercrime and its Policing. American Journal of Computer Science and Engineering Survey. 2020; 8(10):14.
30. Soham Shah, MA Lokhandwala, et al.Decoding Farm Laws. International Journal of Scientific Research and Engineering Development. 2021; 4(2):590-595.
31. Hong J (2012) the state of phishing attacks. Communications of the ACM 55: 74–81. 2. Singer PW, Friedman A (2014) Cybersecurity: What Everyone Needs to Know. 1st Eds, Oxford University Press.
32. Krombholz K, Hobel H, Huber M, et al. (2015) Advanced social engineering attacks. J Inf Secur Appl 22: 113–122.
33. Ducklin P (2020) Phishingové triky aneb 10 nejběžnějších podvodů roku 2020 (Phishing tricks or the 10 most common scams of 2020). IT'S SYSTEMS. Available from: https://www.systemonline.cz/it-security/phishingove-triky.htm
34. Becton L (2020) The Importance of Digital Literacy in K-12, Available from: https://www.educationcorner.com/importance-digital-literacy-k-12.html
35. Parsons K, Butavicius M, Delfabbro P, et al. (2019) Predicting susceptibility to social influence in phishing emails. Int J Hum-Comput St 128: 17–26
36. Lin T, Capecci DE, Ellis DM, et al. (2019) Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. ACM T Comput-Hum Int 26: 1–28.
37. Adewumi OA, Akinyelu AA (2016) A hybrid firefly and support vector machine classifier for phishing email detection. Kybernetes 45: 977–994.
38. Sami S, Nauman A, Li Z (2018) Detection of online phishing email using dynamic evolving neural network based on reinforcement learning. Decis Support Syst 107: 88–102.
39. Zhao M, a B, Kiekintveld C (2016) Optimizing Personalized Email Filtering Thresholds to Mitigate Sequential Spear Phishing Attacks. In: Proceedings of 30th Association-for-the-Advancement-of-Artificial-Intelligence (AAAI) Conference on Artificial Intelligence 30: 658–664.
40. Wang J, Li Y, Rao HR (2016) Overconfidence in Phishing Email Detection. J Assoc Inf Syst 17: 759–783. 12. Williams EJ, Polage D (2019) how persuasive is phishing email? The role of authentic design, influence and current events in email judgements. Behav Inform Technol 38: 184–197.
41. Ferreira A, Teles S (2019) Persuasion: How phishing emails can influence users and bypass security measures. Int J Hum-Comput St 125: 19–31.
42. Seifollahi S, Bagirov A, Layton R, et al. (2017) Optimization Based Clustering Algorithms for Authorship Analysis of Phishing Emails. Neural Process Lett 46: 411–425.
43. Canfield CI, Fischhoff B, Davis a (2019) Better beware: comparing metacognition for phishing and legitimate emails. Metacognition and Learning 14: 343–362. 116 AIMS Electronics and Electrical Engineering Volume 5, Issue 1, 93–116.
44. Nowak J, Korytkowski M, Wozniak M, et al. (2019) URL-based Phishing Attack Detection by Convolutional Neural Networks. Aust J Intell Inf Process Syst 15: 60–67
45. Wei W, Ke Q, Nowak J, et al. (2020) Accurate and fast URL phishing detector: A convolutional neural network approach. Comput Netw 178: 107275.
46. DZRO FVT-2, KYBERSILY. Project of faculty research: Cyber forces and resources. University of Defence, Faculty of Military Technologies, Brno, Czech Republic, 2021.
47. Hajgude, J., Ragha, L.: Phish mail guard: Phishing mail detection technique by using textualandURLanalysis.In:2012WorldCongressonInformationandCommunicationTechnolog ies, pp. 297–302 (2012)
48. Marchal,S.,Armano,G.,Grondahl,T.,Saari,K.,Singh,N.,Asokan,N.:OFf-the-Hook: AnEfficient and Usable Client-Side Phishing Prevention Application. IEEE Trans. Comput. 66(10), 1717– 1733 (2017)
49. Whittaker, C., Ryner, B., Nazif, M.: Large-Scale Automatic Classification of Phishing Pages4. Deng, L.: A TutorialSurvey of Architectures, Algorithms, andApplications for DeepLearning. APSIPA Trans. Signal Inf. Process. (2014)
50. Selvaganapathy, S., Nivaashini, M., Natarajan, H.: Deep belief network based detection andcategorization of malicious URLs. Inf. Secur. J. A Glob. Perspect. 27(3), 145–161 (2018)
51. Kitchenham,B.,PearlBrereton,O.,Budgen,D.,Turner,M.,Bailey,J.,Linkman,S.:Systematicliter ature reviews in software engineering – A systematic literature review. Inf. Softw. Technol. 51(1), 7–15 (2009)
52. Basnet, R., Mukkamala, S., Sung, A.H.: Detection of Phishing Attacks: A Machine Learning Approach. In Soft Computing Applications in Industry, pp. 373–383. Berlin, Heidelberg, Springer Berlin Heidelberg (2008)
53. Yuan, X.: PhD Forum: Deep Learning-Based Real-Time Malware Detection with MultiStageAnalysis. In 2017 IEEE International Conference on Smart Computing (SMARTCOMP), pp. 1–2 (2017)

54. Woodbridge, J., Anderson, H.S., Ahuja, A., Endgame, and D.G.: Detecting Homoglyph Attackswith a Siamese Neural Network 10. Saxe, J., Berlin, K.: eXpose: A Character-Level Convolutional Neural Network with Embeddings for Detecting Malicious URLs, File Paths and Registry Keys (2017)
55. Shima, K., et al.: Classification of URL bitstreams using Bag of Bytes (2018)
56. Vazhayil, A., Vinayakumar, R., Soman, K.: Comparative Study of the Detection of MaliciousURLsUsingShallowandDeepNetworks.In20189thInternationalConferenceonComp uting, Communication and Networking Technologies (ICCCNT), pp. 1–6 (2018
57. Epishkina, A., Zapechnikov, S.: A syllabus on data mining and machine learning with applications to cybersecurity. In 2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC), pp. 194–199 (2016)
58. Zhang, X., Zeng, Y., Jin, X.-B., Yan, Z.-W., Geng, and G.-G.: Boosting the phishing detectionperformance by semantic analysis. In 2017 IEEE International Conference on Big Data (Big Data), pp. 1063–1070 (2017)
59. Vanhoenshoven, F., Napoles, G., Falcon, R., Vanhoof, K., Koppen, and M.: Detecting maliciousURLs using machine learning techniques. In 2016 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 1–8 (2016)
60. Chen, W., Zhang, W., Su, Y.: Phishing Detection Research Based on LSTM Recurrent NeuralNetwork, pp. 638–645. Springer, Singapore (2018)
61. Zhang,J.,Li,X.:PhishingDetectionMethodBasedonBorderline SmoteDeepBeliefNetwork,pp. 45–53. Springer, Cham (2017)
62. Yi, P., Guan, Y., Zou, F., Yao, Y., Wang, W., Zhu, T.: Web Phishing Detection Using a Deep Learning Framework. Wirel. Commun. Mob. Comput. 2018, 1–9 (2018)
63. Aksu, D., Turgut, Z., Üstebay, S., Aydin, M.A.: Phishing Analysis of Websites Using Classification Techniques, pp. 251–258. Springer, Singapore (2019)
64. Zhao, J., Wang, N., Ma, Q., Cheng, Z.: Classifying Malicious URLs Using Gated RecurrentNeural Networks, pp. 385–394. Springer, Cham (2019)