VOLUME - 12, ISSUE - 04, APRIL - 2023 • PRINT ISSN No. 2277 - 8160 • DOI : 10.36106/gjra

Original Research Paper

Technology

CYBER PHISHING AND USE OF MULTI FACTOR AUTHENTICATION TO REDUCE ITS RISKS.

Ashta Siddhi Nagar Amity law school, Lucknow.

Dr Arvind Kumar Singh Assistant professor, Amity law school Lucknow.

ABSTRACT

With the rapid development and innovation in technology, the use and ease of internet access has taken place throughout the world, bringing cyber threats and crimes along with it. As more and more people rely on the internet for communication, commerce, and entertainment, the number of potential targets for cybercriminals has also increased. Cyber-crimes are increasing at an expeditious rate and the global cyber security is facing major threats.
One of the major cyber-crime is cyber phishing. Cyber phishing is a sort of online fraud and cyber security breach that includes duping people or organisations into giving over personal data, such as usernames, passwords, and credit card numbers. In order to trick recipients into clicking on links or downloading attachments that contain malicious software or leading them to a fake website designed to steal their information, phishing attacks typically involve sending emails or messages that appear to be from a reliable source, such as a bank, social media platform, or e-commerce site.
The use of multi factor authentication can be harnessed in order to curb the attacks of phishers. Multi-factor authentication (MFA) is a security mechanism which users to provide two or more authentication factors to verify their identity when logging in to an account. These can typically include something the user knows or is included in their knowledge (such as a password or PIN), something they have or which they possess (such as a physical token or smart card), or something they are or which is bodily attached to them (such as a biometric characteristic like a fingerprint or facial recognition). By creating multiple forms of authentication, MFA makes it much harder for attackers to gain access to user accounts, even if they have obtained the user's password or other personal information through phishing or other means.

KEYWORDS : *cyber crime, cyber phishing, remote access software, multi factor authentication.*

RESEARCH METHODOLOGY

The main source of data for this non-empirical, doctrinal research article will be secondary sources. To substantiate the arguments presented in this study, secondary sources such books, journals, research papers, and newspapers will be consulted.

LITERATURE REVIEW

This paper reviews the literature about the cyber phishing attacks and use of multi factor authentication to reduce its risks. The review aims to showcase how cyber criminals use remote access software to dupe the victims by pretending to be an authorised entity.

RESEARCH PROBLEM

This paper aims to shed light on the various types of cyber phishing attacks and how people become victim of such attacks.

RESEARCH OBJECTIVE

To showcase how multi factor authentication can reduce the likelihood of successful cyber phishing attacks

INTRODUCTION

The word "phishing" refers to the act of data fishing by cyber attackers; the "ph" stands for the sophisticated techniques they employ to differentiate their behaviour from less sophisticated fishing. As these con artists set up "hooks" in the hopes of drawing some "bites" from their targets, it is obvious that the name "phishing" is a variant of the phrase "fishing."

Cyber phishing is a type of online scam or fraud in which an attacker sends a deceptive message or communication (often via email, text message, or social media) that appears to be from a such source that proves to be authentic, such as a financial organization, or a bank, a government institution, or a reputable company. Commonly, the message which is delivered contains a malaware in the link or file that, when clicked or viewed, can result in the loss of private or sensitive data or any important information including passwords, credit card or debit card details, or social security number such as pan card or aadhar card. Cyber phishing has become a common technique used by cybercriminals to trick individuals into divulging confidential information or downloading malicious software onto their devices so that some financial gain can be made to the criminals.

A study has defined cyber phishing as "a fraudulent activity that involves the creation of a replica of an existing web page to fool a user into submitting personal, financial, or password data" According to this, by providing the user harmful links that direct them to a phoney website, phishing is an effort to fool or defraud a person into giving confidential information, such as bank account and credit card data.

The origins or the history of cyber phishing dates back to the early days of the internet when email first became widely used as a means of communication. The first documented case of phishing occurred in the mid-1990s, when scammers targeted AOL users with a fake email that appeared to be from the company's billing department. The email asked users to verify their billing information by clicking on a link, which then led them to a fraudulent website where they were asked to enter their personal and financial information. The phishers would pretend to be an AOL administrator and remind the victim that they needed to update their credit card and login details due to a billing issue.

Since then, phishing has evolved and become more sophisticated, with attackers using increasingly convincing methods to lure victims into disclosing their sensitive information. Today, phishing attacks can take many forms, including emails that appear to be from legitimate sources, fake social media accounts, and fake websites that mimic legitimate ones. Cybercriminals use a variety of tactics to make their messages and websites look legitimate, such as using logos and branding that are similar to the real thing, and creating URLs that are very similar to legitimate ones. Phishing attacks have become a major concern for individuals and organizations alike, and are a significant threat to online security.

TYPES OF CYBER PHISHING

- **Email phishing:** This is the most prevalent kind of phishing assault, where the perpetrator sends the target a misleading email while frequently impersonating a trustworthy source like a banking organization, social media site, or e-commerce website. The email typically asks the recipient to open a file or link to a phoney website that downloads adware onto the victim's computer.

- **Spear phishing:** This is a targeted phishing attack that is aimed at specific individuals or groups, such as employees of a particular company or members of a specific organization. The attacker researches their targets and customizes the phishing message to make it appear more convincing.
- According to data from the RBI, banks lost more than Rs 12,000 crore due to frauds in 2014–15, an increase from Rs 7,542 crore the previous year. Between April 2011 and September 2014, banks recorded 27,614 credit card-related forgeries and an additional 3,835 debit card-related frauds. Particularly when you factor in an extra 1,969 instances of fraud connected to online banking, the figures appear to be too big to disregard.
- **Whaling:** This is a type of a phishing attack where the targets are high-profile individuals, such as CEOs or government officials, with the aim of stealing sensitive corporate or government information. It is highly organized form of cyberphing.
- **Smishing:** This kind of phishing assault uses text texts to carry out its operations. The perpetrator requests that the victim click on a link or input their confidential information in a fake message that appears to be from a reputable source, like a bank or delivery service.

A total of 9, 7, and 19 ransomware incidents involving government organisations were noted during the years 2020, 2021, and 2022, respectively, according to information reported to and tracked by the Indian Computer Emergency Response Team (CERT-In), as per Rajeev Chandrashekhar, Minister of State for Electronics and IT**.** Additionally, throughout the years 2020, 2021, and 2022, there were 59, 42, and 50 instances of website hacking against Ministries/ Departments of the Central Government and of State Governments, as well as 77, 159, and 246 instances of phishing and smishing against government institutions.

- **Vishing**: vishing includes cyber phishing done over the phone. The attacker acts as a trusted source, such as a banking institution or government agent, and tries to trick or fraud the victim into revealing their personal or financial information.

In 2022, For 33-year-old Lokesh Kardam, a vishing episode has made phone banking a nightmare. Kardam received a call from an unknown caller professing to be a bank official informing him that his ATM card had been stopped. He was instructed to disclose his card number and the three-digit CVV (card verification value) number located on the rear of the card in order to have it unblocked. Following that, he was prompted to provide his OTP, at which point 22,000 rupees vanished from his bank account.

- **Clone phishing:** This method of phishing involves making a fake version of an authentic email or website in order to take the victim's money or confidential information. A malicious link or file is present on the duplicated communication or webpage, which otherwise resembles the original.

TECHNIQUES USED BY CYBER PHISHERS

Phishers use a variety of techniques to conduct cyber phishing attacks. Some of the most common techniques include:

- **Email Spoofing:** Phishers use email spoofing to make an email appear as if it is from a legitimate source. They use techniques to manipulate the email header to make it look like the email is coming from a trusted source.
- **Deceptive URLs:** Phishers use deceptive URLs to trick users into clicking on a link that appears to be legitimate, and after clicking it, leads to a fake site which steals the personal information of the user.
- **Social Engineering:** Phishers use suchtechniques to manipulate people into providing personal information or performing an action that benefits the attacker. This can include using emotional appeals, creating a sense of urgency, or pretending to be a trusted authority figure.
- **Malware:** Malware, such as viruses or trojans, can be used by phishers to infect a user's machine and steal confidential data. A malicious website or email file can accomplish this.
- **Spear phishing**: A targeted phishing assault that is directed at a particular person or business is known as spear phishing. Phishers will compile data from social media and other sources to build a customised attack that has a higher chance of succeeding.

Overall, it is critical to be conscious of these tactics and to take precautions against phishing assaults. Some of these precautions include being wary of unsolicited emails and double-checking any links or files before clicking on them.

STATISTICS RELATED TO CYBER PHISHING

According to a recent report by Group-IB, India was ranked third globally and topped in Asia-Pacific area among the 111 nations hit by a global cyberattack in which a group of fraudsters stole passwords through a coordinated phishing campaign. Amazon credentials, which made up 32% of the stolen passwords in India during the final 10 months of 2021, were among the passwords that hackers most regularly acquired, followed by PayPal at 17%. According to researchers, the value of the compromised card information and stolen data on the black market was around $5.8 million USD. Data from the National Crime Records Bureau (NCRB) show that 52,974 cybercrimes were reported in 2021. In compared to the prior year, the statistics climbed by over 6%.

Like many other countries, India is seeing a rise in hacking. There were 208,456 recorded cyber-related offences in 2018. With 212,485, there were more cybercrimes recorded in the first two months of 2022 than there were in 2018.

Through the epidemic, the numbers increased even more dramatically, with the number of reported crimes increasing from 394,499 in 2019 to 1,158,208 in 2020 and 1,402,809 in 2021. India saw a 15.3% rise in cybercrime between Q1 and Q2 2022. Additionally, in recent years, there have been a growing number of hacks on Indian websites. Around 17,560 websites were compromised in 2018. A further 26,121 websites were compromised in 2020.

Lucknow was ranked number two in the crime rate and 3rd in the absolute numbers, according to a report by NCRB (National Crime Records Bureau). A total of 962 cyber-crimes were reported in the city in 2018. In terms of crime rate, Lucknow ranked second with 33.2 cases per lakh population.

USE OF REMOTE ACCESS SOFTWARE ACTING AS A CATALYST FOR CYBER PHISHING

A form of software called remote access software enables users to connect to and manage a computer or network from a distance. With the use of this technology, people and businesses may work from any place, interact with coworkers in other cities, and have access to resources that aren't nearby. Examples of these software products include: Microsoft Remote Desktop is remote access software that enables users to connect to networks and computers running Windows from any platform. It has functions including clipboard redirection, audio redirection, and remote printing. somewhere on the planet. It has capabilities including file sharing, screen sharing, and remote printing.

Using AnyDesk, users may connect to networks and computers from any location in the globe. AnyDesk is a remote access programme. It has functions including remote printing, file sharing, and multi-platform support.TeamViewer is a well-known remote access programme that enables users to connect to computers and networks from any location in the globe. It has functions like remote printing, screen sharing, and file transfer.

IT professionals frequently use remote access software to manage and troubleshoot computers and servers from a centralised location, support specialists to assist clients and colleagues with technical problems, and telecommuters to work from home or other remote locations.

One way attackers can use remote access software to launch phishing attacks is by tricking remote workers into downloading and installing malicious software on their computers. This can be done through fake emails, social media messages, or other types of communication that appear to be legitimate. Another way attackers can use remote access software to launch phishing attacks is by impersonating legitimate remote access services. For example, attackers may create fake login pages that look like the real thing in order to trick users into entering their login credentials.

In a recent phishing attack in Lucknow, a 40 year old man got duped of 2.5 lakh rupees. He received a call that he had an arrear on his electricity bill, and if he does not pay it, his connection would snapped off. The man who called claimed to be an official of UPPCL, he asked him to install Anydesk app to see whether the payment was made and asked for 5 rupees as service charge to be made. Within few minutes 2.5 lakh rupees were gone from his bank account.

A similar incident happened with another 50 year old man from krishna nagar where he was asked to pay 10 rupees as service charge and got duped of Rs.75,800.

A 90 year old NRI, who wanted to get his car insurance renewed, surfed on the internet for number of regional transport office and the receiver who asked him to install anydesk app and pay a service charge of rupees 10 and within some time 5 lakhs were deducted from his account.

To mitigate the risks of cyber phishing when using remote access software, it is important to use strong passwords and multi-factor authentication, keep software and security tools up to date, and be wary of suspicious emails or messages. Additionally, organizations can provide training and education to employees to help them recognize and avoid phishing attacks.

USE OF MULTI FACTOR AUTHENTICATION TO REDUCE THE LIKELIHOOD OF SUCCESSFUL PHISHING ATTACKS AGAINST USERS.

In order to access a system, application, or service, users must provide two or more forms of authentication using the security method known as multi-factor authentication (MFA). By asking the user to submit more information than just a password, MFA aims to strengthen the security of the authentication process.

Typically, the three authentication elements are:

- Information that the user is aware of, including a password, PIN, or the solutions to security questions
- Something the user is, like biometric information like a fingerprint or face recognition;
- Something the user owns, like a mobile phone;
- A physical token, like a smart card or USB key.

MFA makes it more difficult for attackers to obtain unauthorised access to a system or account by requiring two or more sources of authentication. Even if a user's password were to fall into the wrong hands, an attacker still needs the extra factor(s) of authentication to get access. Online banking, email, and social networking platforms are just a few of the applications and sectors that frequently employ multi-factor authentication (MFA).

In cyberattacks, attackers frequently use poor or stolen credentials to gain access to accounts and networks. MFA can help stop these assaults by demanding a second authentication mechanism, such as a fingerprint scan or one-time pass provided to a mobile device.

Criminals frequently exploit weak or stolen passwords in cyberattacks to access accounts and networks. By requiring a second authentication method, such as a fingerprint scan or one-time code given to a mobile device, MFA can aid in preventing these attacks. Cybercriminals will find it more challenging to access accounts as a result, even if they have managed to get their hands on the user's passcode.

MFA can also aid in defending against phishing attempts, in which criminals create phoney login pages in order to obtain user credentials. Without the second factor of authentication, the attacker would not be able to access the account even if a victim falls for a phishing hoax and inputs their password.

MFA also has the ability to identify and stop unauthorised access to networks and applications. MFA can identify suspicious behaviour or odd login attempts, such as attempts to login from an unfamiliar device or location, by demanding several forms of authentication.

Only by using multilayer authentication procedures is there a potential to lessen criminals' attempts at phishing.

WAYS TO ADOPT TO BE PROTECTED AGAINST THE RISKS IMPOSED BY CYBER PHISHING

Inorder to safeguard organizations and individuals here are some ways to minimize the risk of falling victim to a cyber phishing attack:

Educate both yourself and your staff: Educating yourself and your staff about phishing and how to recognise it is the first step in preventing a cyber phishing assault. Phishing emails may look to be from a reliable source and frequently include suspicious links or attachments. You may lessen the possibility of someone falling for a phishing attempt by teaching yourself and your staff to be more watchful.

Use anti-phishing software to install: Phishing attempts may be recognised and avoided with the use of anti-phishing software. Incoming emails are routinely checked by this programme for suspicious content, and any emails that appear to be phishing attempts are blocked.

Update software regularly: Phishing attempts frequently make use of software flaws. You may lessen your chance of being a phishing victim by maintaining current software.

Use multi-factor authentication: This security feature forces users to supply many different forms of identity before gaining access to an account. You can make it far more difficult for hackers to access your accounts by utilising multi-factor authentication.

Be careful while giving out personal information: because phishing attempts sometimes focus on getting hold of passwords or credit card details. You may lessen your chance of being a phishing victim by being cautious with your personal information and only giving it to dependable sources.

Use strong passwords: Protecting your online accounts requires strong passwords. Make sure to use a complicated combination of letters, numbers, and symbols in your passwords. Refrain from using the same password across numerous accounts, and change it frequently.You can lessen your chance of being a victim of a cyber-phishing assault by heeding the advice in this article. Though no security mechanism is flawless, it's crucial to keep in mind that you should always use caution and vigilance when browsing the internet.

CONCLUSION

In conclusion, cyber phishing is a threat to , companies, and organisations all over the world. Attackers employ a variety of strategies to trick their victims into disclosing private information like passwords and financial information. The use of multi-factor authentication (MFA) in all accounts and systems is one of the best strategies to defend against phishing attempts.

MFA is a security procedure that asks users to submit other authentication elements in addition to their login and password, like a fingerprint scan or a one-time passcode. Even if attackers are successful in obtaining the user's password via a phishing assault, this makes it far more challenging for them to access accounts.

In summary, while phishing attacks remain a prevalent threat, implementing multi-factor authentication can significantly reduce the risk of successful attacks and safeguard personal and sensitive information. It is crucial to stay vigilant and adopt best practices to protect against cyber threats continually.

In conclusion, even if phishing attempts are still a serious concern, using multi-factor authentication may greatly lower the likelihood that an attack will succeed and protect confidential and personal data. In order to continuously guard against cyber dangers, it is imperative to exercise caution and use best practises.

REFERENCES

1. Lance James, 2005. Phishing Exposed. Syngress, Canada
2. Merwe, A. v. d., Marianne, L., and Marek, D. (2005). "Characteristics and responsibilities involved in a Phishing attack, in WISICT '05: proceedings of the 4th international symposium on information and communication technologies" .Trinity College Dublin.
3. https://www.hindustantimes.com/india/phone-banking-fraud-hits-thousands-tricksters-deal-rs-12-000-cr-blow/story-AP7DdpYdoHwX0UADrQnxRM.html
4. https://www.tribuneindia.com/news/nation/cyber-attacks-on-govt-department-rising-151-hacking-492-phishing-cases-in-3-years-479404
5. https://www.hindustantimes.com/india/phone-banking-fraud-hits-thousands-tricksters-deal-rs-12-000-cr-blow/story-AP7DdpYdoHwX0UADrQnxRM.html
6. https://www.hindustantimes.com/cities/mumbai-news/india-third-most-targeted-country-by-phishing-campaign-report-101670179300520.html
7. indiatoday.in/technology/features/story/cyber-fraud-incidents-rising-in-india-how-to-file-a-complaint-online-on-cyber-crime-portal
8. https://timesofindia.indiatimes.com/city/lucknow/cyber -crooks-preyed-on-1-resident-every-10-hours/articleshow/73209287.cms
9. https://timesofindia.indiatimes.com/city/lucknow/cyber-con-dupes-man-of-rs-2-5-lakh-over-power-dues-in-up/articleshow/98789537.cms?from=mdr
10. https://timesofindia.indiatimes.com/city/lucknow/who-will-pull-the-plug-cons-again-dupe-man-in-name-of-electricity-bill/articleshow/97045061.cms
11. https://www.phishing.org/10-ways-to-avoid-phishing-scams