International Journal of Safety and Security Engineering
Vol. 13, No. 2, April, 2023, pp. 333-340
Journal homepage: http://iieta.org/journals/ijsse

An Investigation on Vulnerability Analysis of Phishing Attacks and Countermeasures

Ganga Abhirup Kothamasu, Sree Keerthi Angara Venkata, Yamini Pemmasani, Senthilkumar Mathi*

Department of Computer Science and Engineering, Amrita School of Computing, Coimbatore 641112, Amrita Vishwa Vidyapeetham, India

Corresponding Author Email: m_senthil@cb.amrita.edu

https://doi.org/10.18280/ijsse.130215

Received: 22 February 2023
Accepted: 3 April 2023

Keywords:
authentication, phishing, cybercrime, social engineering, security, attack

ABSTRACT

A great venue for communication amongst regular people is the internet. Many efficient communication methods are available online, such as email, mailing lists, discussion forums, chat services, online conferencing, and blogs. Social networking websites like Facebook, Instagram, and Twitter have recently entered the picture. People who want to steal personal information have discovered a technique with the least chance of getting detected without meeting the target, known as phishing. Phishing is a cybercrime that targets passwords, banking information, credit card information, and personal identification through emails, phone calls, and texts. Mostly, online identity theft takes the form of phishing. The phisher uses social engineering to obtain the victim's account and personal information. A person, a group, or a cluster within a group of people might be the target. In the modern-day, cybersecurity is a major worry to provide a realistic experience of phishing attacks. The present paper investigates and analyses various phishing tools that can simulate such attacks. In addition, the paper investigates the prevention methods and countermeasures. It also examines the kinds of phishing tools, like Zphisher, CamPhish, and PyPhisher, being used to ensure that even people apart from experts can be aware of what a phishing attack is and how to alert others about the risk they pose and how to be prepared for them associated with the recent threats of Crelan Bank and Uber.

1. INTRODUCTION

Faulty authentication is when a platform or program online has flaws or vulnerabilities that allow hackers to log in without being detected and access all the user's capabilities. The different sorts of these inbuilt flaws are weak session management and weak credential management.

Session management flaws can only be understood after familiarising how browsing and online authentication typically operate. Each user interaction with a network on social networking websites or online betting portals is logged and added to a web session that the web application may track. The web application provides the user with a session identity for each visit. This identity is necessary for the application to interact with the user and answer requests. Stealing or using unauthorized users' credentials to access the program is also possible. As a result, managing credentials is crucial for cybersecurity. A web application must ensure that passwords like *1234* or *password* are not permitted. If such passwords are permitted to be used, credential management is weakened. It is a sort of failed authentication if the online application cannot defend users against hackers who force their way in using stolen or compromised credentials.

Hackers might target one by combining information from many sources. With the information they've discovered, they may design unique phishing techniques. They have successfully developed harmful malware targeting phishing apps [1]. Hackers phish to trick users into disclosing their login credentials by giving them URLs to websites that seem just like online applications. Phishing begins with an email or another kind of contact intended to help target the victim [2]. The message appears as though it has come from a reliable source. Victims are tricked by their personal information to spam websites. Malware may also possibly be transferred into the target's machine. Phishing attacks are matched by 482 CVE records (the year 2004 to the present 2022).

According to a recent report, targeted phishing attacks affected over 90% of firms in 2019. Of these, 88 percent reported spear-phishing assaults, 83 percent voice phishing (also known as "Vishing"), 86 percent social media attacks, 84 percent SMS/text phishing (also known as "Smishing"), and 81 percent malicious USB drops. Phishing assaults increased from 76 percent in 2017 to 83 percent in 2018, according to the 2018 Proofpoint1 annual study, with all phishing attacks occurring more frequently than in 2017. The second quarter of 2019 saw a significant increase in phishing attacks reported compared to the first three quarters. According to a study from the anti-phishing working group, this figure was greater in the first quarter of 2020 than in the prior year, concluding that phishing attacks are rising [3].

2. LITERATURE SURVEY

There are several ways to recognize phishing assaults. The creativity of the new phishing assaults requires periodic revisions of these attacks. The heuristics approach attempts to comprehend the study of phishing websites and identify assaults based on several characteristics, including the domain name, domain age, spelling mistakes, picture source, etc. [4].

Different machine learning methods, such as the random forest algorithm, Support vector machine (SVM), swarm intelligence, genetic algorithm, etc., are employed in the machine learning approach. SVM has been successfully utilized to address several classification issues [5]. The blacklist strategy involves adding untrusted URLs or a list of prohibited websites to the blacklist [6]. The URL being typed right now is compared to the malicious defined list.

Additionally, the contents are examined, and if the URL content matches, the URL is banned, and the user is warned. The blacklist also includes a total phishing page count [7]. Fuzzy logic-based data mining algorithms are utilized in the fuzzy rule-based technique to experiment and identify phishing websites [8]. The cantina-based technique employs both term frequency and inverse document frequency (TF-IDF) for identifying phishing sites. The TF-IDF retrieval algorithm is frequently used for document classification and comparison [9]. The image-based method compares legitimate and phishing websites based on visual similarities [10].

Phishing attempts are sometimes challenging to spot since they frequently seem like spam or pop-up windows. Once the attacker has your personal information, they can use it for identity theft and other crimes, damaging your excellent credit. Since phishing and cyber-attacks are the sneakiest ways to steal someone's identity, one must learn about the many phishing attempts and how to avoid them [11, 12].

The primary focus is to examine phishing attacks in cyberspace and any malicious web content that operates inside the browser [13]. It is impossible to scan for viruses in downloaded files that use third-party PC software and include viruses. For instance, if a word document is downloaded to the PC, the VM cannot handle it since it employs no web-based tools. In the study [14], the "Anti Phishing Simulator" program, which provides information on the phishing detection issue and how to recognize phishing emails, was created as part of it. This program examines the mail's contents to identify phishing and spam emails. By using a Bayesian method, spam terms that have been added to the database are categorized.

A brand-new hybrid deep learning model is suggested to recognize phishing assaults [15]. It has two parts: a convolutional neural network (CNN) and an autoencoder (AE). The AE is used to rebuild features that improve the connection between the characteristics. The results of the studies reveal that the model has a mean accuracy of over 97.68 per cent in detecting phishing attempts, but it also has a high degree of generalizability and can do so in an acceptable time frame. The work in the study [16] analyses emails using data mining techniques and helps avoid phishing scams. This study developed an architectural approach that uses naïve Bayesian classification to accurately distinguish between fraudulent and authentic emails. The suggested algorithm attempts to shield users from disclosing their private information by working in steps to detect fraudulent emails.

A secure authentication mechanism uses QR codes and secret key exchange [17]. This authentication system contains a mobile application just for authentication, eliminating the need to enter website login information and making it more resistant to phishing. The work [18] examines many phishing attempts, some of the most recent assault evasion methods, and anti-phishing strategies. This review helps users practice phishing avoidance by increasing their awareness of those phishing methods. Here, a hybrid phishing detection method with quick response times and excellent accuracy is also discussed.

The investigation [19] suggests an AI-based, self-aware, self-defending system that delivers cogent responses. Send responses from mail servers produced by algorithms to make it harder for spammers. Additionally, use a language model trained using LSTM to create phrases in natural language based on the context of the email to make the answers unique from each other and authentic to circumvent spammers' easy match filtering of emails. A comparison is given between the traditional machine learning method of logistic regression using bigram and the deep learning methods of convolution neural network and CNN-LSTM as structures used to detect bad URLs for categorizing phishing URLs, CNN-LSTM demonstrated the highest accuracy, at roughly 98 percent [20].

In paper [21], a device setup method generates authentication credentials automatically from device settings. Compared to conventional authentication methods like passwords, the increased speed demanded by the technique is tolerable, and the security offered is reasonable. Detailed security and threat research showing that this technique neutralizes 9 out of 10 detected risks highlights the strategy's security advantages. In the paper [22], to determine the important data protection strategy to stop unauthorized people, the suggested security methods may be used with SSL, digital signatures, network security, etc.

The paper [23] provides a thorough analysis of research that use machine learning (ML) and natural language processing (NLP) techniques to spot phishing emails. Subsequently, the paper [24] overviews cyber security's forecasting and prediction techniques. First, four key responsibilities are covered: attack projection and intention recognition, intrusion prediction, predicting the cybersecurity state of the whole network, and attack projection and intention recognition, which require projecting the attacker's next move or intents. Theoretical underpinnings are frequently shared and complementary across methods and approaches to tackle these issues. Compares and contrasts strategies based on continuous models like time series and grey models with those based on discrete models like attack graphs, Bayesian networks, and Markov models.

The paper [25] emphasizes the development, propagation, and operation of malware, electronic system assaults, phishing websites, cyberbullying, etc. After thoroughly examining the numerous cases, a conclusion and the development of technologies like Honeypots and certain preventive methods to stop cybercrime were reached. All facets of society are now digitally connected due to global development and digitization using the internet of things. Nowadays, banking involves marketing and internet financial transactions. Cloud computing is used in business, yet it is also subject to several hazards, including responsibility and data ownership. The article concludes India's terrible state and makes predictions regarding the country's future regarding cyber security.

3. METHODOLOGY

The attacker makes their false websites, for instance, a fake Facebook website with a phishing.php file that would gather all kinds of information and an index.html page. Without logging in, the attacker visits the Instagram page. The attacker searches for word action to locate a connection as follows.

Action= Login attempt=1 at https://www.instagram.com/login.php

The attacker next registers for a free hosting account on a site like http://www.get-new-followers.com. The phishing website was then constructed when the attacker submitted a PHP file and an HTML page bearing his name. Now the attacker may begin phishing.

3.1 PyPhisher

Python's PyPhisher is the best phishing tool available. It is a Python-based tool used for creating phishing pages. The tool includes several well-known websites, including Facebook, Twitter, Instagram, GitHub, Gmail, and many others. The PyPhisher phishing tool has 65 templates. The credentials retrieved after the attack are recorded in the usernames.txt file, and Ip addresses are stored in ip.txt.

3.2 Zphisher

Zphisher is an effective open-source phishing tool. This tool allows you to engage in phishing (in a wide area network). This tool can obtain credentials like a user id and password. It provides phishing templates of web pages for 18 well-known websites, including Facebook, Instagram, Google, Snapchat, Microsoft, and others. The Zphisher phishing tool has a total of 34 templates of web applications that look mostly the same as the original platforms. When the victim falls for the fake templates and gives their credentials, those are directly stored in the usernames.txt file. Zphisher also supports multiple phishing attacks, including tab nabbing, credential harvesting, and phishing over social media.

3.3 CamPhish

CamPhish is a camera phishing toolkit and a method for photographing the target's front-facing phone camera or computer webcam. To create a URL one provides to the target, CamPhish hosts a false website on an internal PHP server. If the target agrees, the website requests their camera access, and this tool then takes screenshots of the target's gadget. The CamPhish phishing tool has two port forwarding options, Ngrok and Serveo.net. It generates a direct link the user sends to the victim to access the victim's webcam and get cam shots. These pictures that are retrieved are stored in the CamPhish folder directly.

Cybercriminals often use the tools stated above for illegal activities, which can result in serious data loss. These tools are created to carry out phishing attacks. It's crucial to stay alert and take precautions to protect your online accounts and confidential information.

4. RESULT ANALYSIS

The current section discusses the result analysis. As shown in Table 1, the PyPhisher and Zphisher phishing tools are only tested on Linux and Android. At the same time, the CamPhish tool is tested on Linux, Mac, and Android.

Table 1. Platforms with tested tools

Phishing tools	PyPhisher	Zphisher	CamPhish
Linux	Yes	Yes	Yes
Mac			Yes
Windows			
Android	Yes	Yes	Yes

Table 2 lists all the dependencies, features, usage, port forwarding options, and data that a specific tool can record. When comparing the three tools with their templates, PyPhisher has around 65 templates that give users a broad range of options. PyPhisher phishing tool takes more time when compared with the other two tools and does an attack in around 64 seconds.

Table 2. Comparisons of tools

Phishing tools	PyPhisher	Zphisher	CamPhish
Requirements	Python(3), PHP, Curl, Unzip, Wget, 100MB-storage.	PHP, Wget, Curl, OpenSSH, git	PHP, Git, OpenSSH, Wget
Port Forwarding Options	Ngrok, Cloudflare	Local Host, Ngrok, Cloudflare	Ngrok, Serveo.net
Attack Time	64 seconds	26 seconds	40 seconds
Templates	65	34	3
Usage	Easy	Easy and User-friendly	Easy
Data	Get an IP address and many other details, along with login credentials.	Get an IP address with login credentials.	Get an IP address with cam shots (webcam access)

The financial institutions targeted 23.6 percent of all phishing attacks during the first quarter of 2022. Additionally, webmail and web-based software services accounted for 20.5 percent of assaults, making them the two most often targeted sectors for phishing during the reviewed quarter [26].

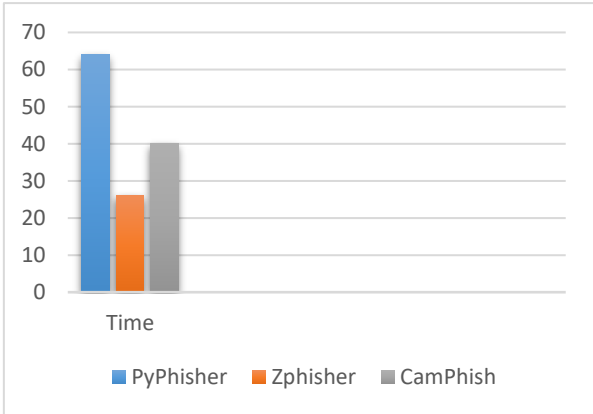

Figure 1. Time analysis of tools (in seconds)

As shown in Figure 1, Zphisher is the fastest phishing tool and does an attack in 26 seconds. Followed by the CamPhish phishing tool, which does the attack in 40 seconds.

5. PREVENTION METHODS AND COUNTERMEASURES

Even though there are many prevention strategies, the first main measure and approach are to improve awareness of phishing. Hackers can easily fool people and make them victims of this attack at ease. Therefore, all individual users

and workers must know about dealing with and identifying these suspicious emails and report them immediately to their specific authorities. Thousands of people log into their social media handles every day. Phishing in this sector has become very popular and proved to be one of the favourite mediums to trap its victims. Whatever it may be, some countermeasures are mentioned as follows.

- Installing anti-virus or anti-spam software can help detect and prevent any unauthorized access. We need to keep it up to date for it to function properly.
- Usage of a unique password for each account must be introduced.
- Social media must never be trusted because our credentials and personal information are sometimes asked for through forms. Sharing all this sensitive information must always be avoided.

5.1 Countermeasures – An investigation

The technical measures by various authors are investigated as follows.

1) Procedures to distinguish the assault after it has been sent off. For example, by checking the web to track down illegal websites. For instance, content-based phishing identification approaches are intensely sent on the web. The highlights from the site components like the picture, URL, and text content are dissected by Rule-based approaches and AI/ML that analyze the presence of exceptional characters (@), Domain IP addresses, and much more [27]. Fuzzy Logic has additionally been utilized as an enemy of the phishing model to assist with grouping sites into authentic or 'phishy' as this model takes care of intervals rather than explicit numeric qualities/values [28] The major benefit of fuzzy logic techniques is the ability to relate the likelihood of phishing emails and websites by using linguistic variables to reflect important phishing characteristics or signs. This model was created and put into use utilizing the incircle fuzzy rule interpolation technique.
2) Ways to prevent the attack from going towards a user's system. Phishing counteraction is a significant stage to safeguard against phishing by obstructing a client from seeing and managing the assault. In email phishing, against spam, programming devices can obstruct dubious messages. Phishers typically send a veritable clone email that hoodwinks the client to open or snap on a connection. Some of these messages pass the spam channel since phishers use incorrectly spelt words. Hence, methods that identify fake messages by checking the spelling and language structure revision are progressively utilized, so it can keep the email from arriving at the client's post box. According to the study [29], a new classification algorithm is based on random forest. The developed method id was PILFER (Phishing Identification by Learning on Features of Email Received). It can identify phishing emails depending on many features like IP-based URLs, number of domains, dots, unmatched URLs. According to a study, PILFER detected 96 percent of phishing emails correctly, with a false-positive rate of 0.1 percent. This intends to achieve an overall accuracy of 99.5 percent.
3) Remedial strategies that can bring down the compromised site, by mentioning the site's Web access Supplier (ISP) to close the fake site to keep additional clients from falling casualties to phishing [30]. ISPs are liable for bringing down counterfeit sites. Eliminating the split between the difference and unlawful sites is a perplexing cycle; numerous substances are engaged in this interaction, from privately owned businesses, self-administrative bodies, government offices, volunteer associations, policing, and specialist organizations. As indicated by the PHISHLABS report and a study, bringing down phishing locales is useful, yet it isn't compelling as these destinations can, in any case, be alive for a long time, ISPs can reduce the number of phishing emails that reach users by up to 90 percent.

5.2 Recent threat of Phishing attacks

Phishing attacks are common these days and are becoming worse over the years rather than completely disappearing. Even though some security applications offer the slightest defences against these small phishing attacks, the tools provided over here are not 100%, and there is a broad chance that many unwanted websites or fraud messages pave their way through. The real-life examples of phishing attacks are as follows.

- Crelan Bank: In this bank, the attacker sent mail to one of the employees acting as CEO, asking the employee to transfer the funds into the account the attacker controls. Thinking that the CEO had sent the mail, the employee transferred huge funds to the attacker's account. This attack happened because of faulty authentication on the domain server side. It led to a huge loss of over 75.6 million dollars. This attack consists of a simple spear-phishing email sent to a senior executive of the company, a member of the financial team, or even a random employee. There have also been occasions where the sender attempted to pass themselves off as a business associate or even a representative of the organization, requesting money be transferred to a certain account to complete a pressing business transaction. To trick upset employees into transferring the money without first double-checking with someone from within the company, the hacker utilized real graphics and a fake domain name.
- Facebook and Google: Between 2013 and 2015, they used Quanta, the Taiwan-based company, as their vendor. The attacker sent a series of fake invoices to both companies imitating Quanta, and both companies paid (100 million dollars) as per the invoice. But later, the scam was identified, and companies acted against the attacker.

Another recent incident that impacted a lot is the massive breach suffered by Uber. The popular ride-hailing company Uber has faced an enormous data breach in which the company fell victim to a general Phishing scam where the attacker fantasized about being someone associated with the company. They then persuaded an employee with many login credentials to get access to the company's internal systems. The company then lost their respect and reputation across the whole world. Thus, one phishing attack can cause great loss. This issue happened on 15 September 2022 and became a massive phishing attack. On 15 September 2022, Uber's internal systems were completely compromised. The attacker figured out how to hack the organization's hacker one account, then

accessed a Leeway account which gave access to the AWS web administrations and even the GCP accounts. Hence, Uber is still investigating the incident; most internal systems were temporarily disabled due to the hack/ phishing attack. On 15 September 2022, an 18-year-old learned to hack Uber through phishing. He (the hacker) had a small blueprint of the organization's inward frameworks and initiated some social strategies to compromise a worker's account. After earning the account credentials, he gained access to the company's internal databases and obtained full control over the company's Amazon Web Services and even the Google Cloud Accounts. An official tweet circulated during the incident is shown in Figure 2.

Figure 2. An official tweet

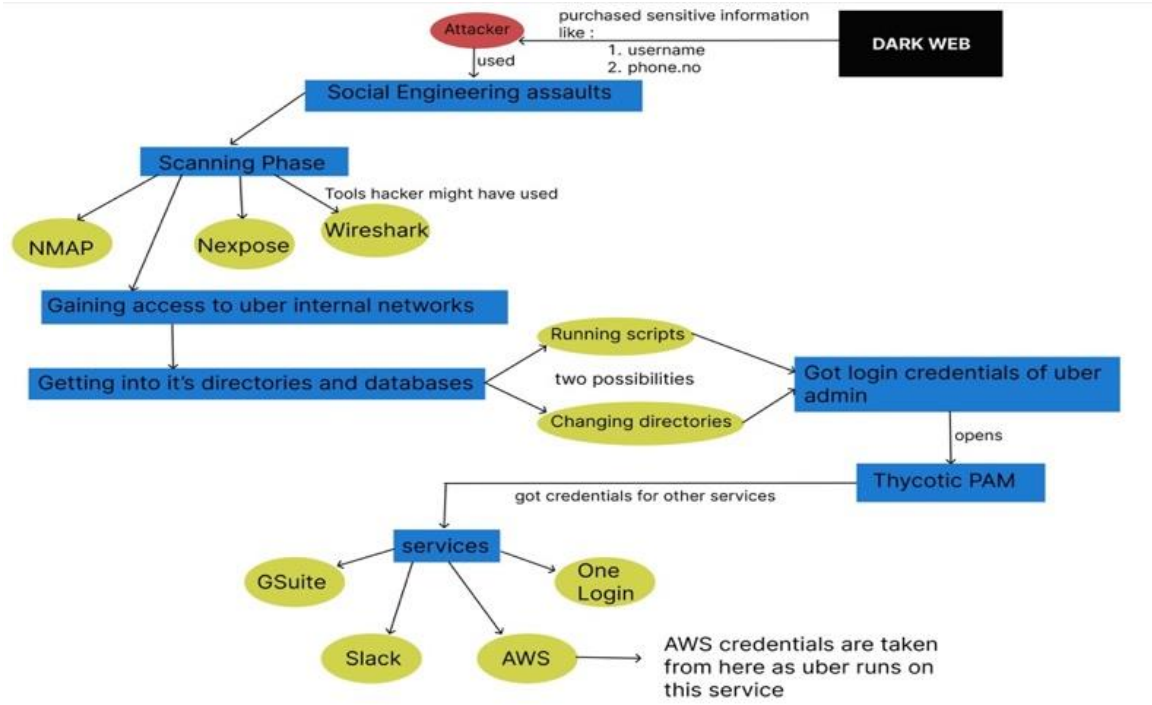

Figure 3. Process flow diagram

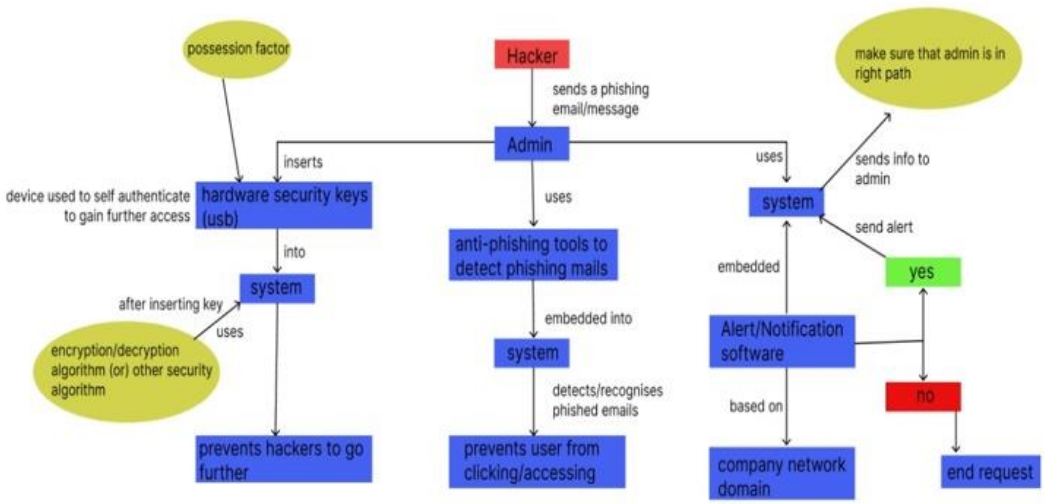

Figure 4. Possible prevention for the UBER attack flow diagram

Firstly, the hacker might have done a brief information search on the victim, which means that he underwent the foot-printing phase and purchased highly sensitive information like username, address and phone number from an online source named DARK WEB, as shown in Figure 3. Almost all sensitive information of many organizations and people is available for a certain amount of money. This being a crucial step, the whole process completely depends upon this. If that information is proven wrong, the hacker fails to proceed further. He then immediately imposed a social engineering assault on his victim. Eventually, the victim's trust was gained and gave him a positive result as the victim finally fell into his trap. All other information related to the company was spilt out, and the hacker finally gained access to the company's database, restricted portals, and internal networks by scanning. NMAP, Nexpose, and Wireshark might have been used to detect input-output packets, open ports, private and restricted ports, Ip addresses and much more. Login credentials of the Uber admin were given out, parallelly giving access to its Thycotic PAM, where the company stores all its passwords in an encrypted form and helps manage their privileges. Thycotic PAM is like a key for hackers to access the whole company. As he had the admin's credentials, he could break into it easily. Finally, he got access to all other services like Slack, AWS and much more.

Whenever the hacker sends a phishing email/message to anyone, there is a high probability that they fall into the hands of the hacker. The possible prevention for the UBER attack flow diagram is shown in Figure 4. Similarly, the admin first sent this and spammed it with many messages to gain trust. There are many ways to prevent this from occurring. Some of the effective methods include as follows.

- Using a hardware device as a security key: when the admin/employee gets a phished email or suspicious message from a third person, it's better not to respond. If he/she decides to access that email or link, they could use a hardware security key, typically a USB. That device could be inserted in the admin's system; it then uses a random encryption/ security algorithm and makes it safe for the system to be accessed/ hacked; it might also help detect suspicious emails. It restricts the third person from hacking.
- Anti-Phishing Tools: This is one of the most revised and traditional methods of detecting spam, suspicious email, and messages. These tools are embedded into the system to recognize unwanted emails and prevent the user/admin from clicking them.
- Using alert/notification software: an alert system is embedded. It ensures the system receives the message from the company's network domain. All the users and officials of the company always communicate through a separate network domain. It keeps the admin on the right path. The admin gets an alert of the whole message and judges it based on location.

The success of phishing attacks can be summarized as follows.

- Techniques used in social engineering: Phishing attacks frequently use social engineering techniques to deceive people into disclosing sensitive information. In the case of the UBER attack, the attackers most likely used a convincing email or website that gave the impression it belonged to a respectable organization to fool UBER personnel into providing their login information.
- Lack of multi-factor authentication: A security feature known as multi-factor authentication asks users to provide a second piece of information besides their password, such as a code delivered to their phone. Multi-factor authentication may not have been in use at UBER at the time of the attack, making it simpler for the attackers to access employee accounts.

5.3 Other countermeasures

The other countermeasures are discussed as follows.

1) Like the security key method, there must be a limit to the number of verified devices. Only the devices assigned permission can access the account and its required sensitive information when there is a limit for the number of devices. By this, if a third-party member tries to access it, he/she would be restricted. If they want to access it, they would only do so through the assigned devices, which are highly secured and encrypted. This method may not be optimal in all situations, but it proves secure.
2) The company must ensure that all its employees or admins undergo strict training, so they won't fall for all the silly tricks the hacker imposes. In contrast to this issue, the company's admin unknowingly fell into the trap of a teen. They must be given at least four to six months of training before their joining date to prevent these small mistakes.
3) Setting a limit to the number of notifications on every admin's device is also a major factor. When an employee or admin is targeted under social engineering hack, the hacker continuously troubles and threatens that person. When some emails or notifications are received, the admin (victim) eventually stops getting those threatening notifications for some time. The company can take this issue immediately after that shoot; on the other hand, the admin would also change his mind and thoughts about those notifications.

The company can provide an encrypted device to all its employees/admins, which generates passwords. Of this, the hacker needs to hack repeatedly to get the correct credentials or information.

5.4 Measures and suggestions to avoid and reduce phishing and network security

1) Implement email authentication: Implement email authentication protocols such as DKIM, SPF, and DMARC to prevent email spoofing and increase email security.

DomainKeys Identified Mail (DKIM): DKIM is an email authentication protocol that verifies the authenticity of an email message by attaching a digital signature to the email header. The signature is created using the sender's private key and is validated by the recipient's email server using the sender's public key.

Sender Policy Framework (SPF): SPF is an email authentication protocol that verifies that an email message was sent from an authorized IP address associated with the sender's domain. SPF records are published in the sender's DNS records and specify which IP addresses are authorized to send emails on behalf of the domain.

Domain-based Message Authentication, Reporting, and Conformance (DMARC): DMARC is an email authentication protocol that builds on DKIM and SPF to provide additional security measures. DMARC enables email receivers to determine the authenticity of an email message by verifying that it passes both DKIM and SPF checks. DMARC also provides guidelines for handling messages that fail authentication checks, such as quarantining or rejecting them.

2) Web Filtering: Implementing web filtering tools can help to prevent employees from accessing known phishing websites and block malicious content from being downloaded onto the network.
3) Conduct regular security audits: By conducting regular security audits, organizations can identify and address vulnerabilities and weaknesses in their IT infrastructure, policies, and procedures and improve their overall security posture. This can help to reduce the risk of security breaches and other cyber threats and increase confidence in the organization's ability to protect sensitive data and assets.

6. CONCLUSIONS

There are various solutions/preventions available, but whenever any solution is proposed to overcome these attacks, phishers always come with the vulnerabilities of the solution to make the attack successful. All these phishers made sure that they used communication media to perform all the restricted activities using fake web pages and spoofed emails. But the average user who falls prey to phishing suffers a terrible loss since they are unaware that their personal information is being used against them for fraud or even that their bank accounts are being raided without their knowledge. So, it becomes crucial to confirm that users have received the essential instruction and information on the dangers of compromised authentication due to phishing scams or poor passwords. It not only destroys one's identity, and it never misses to create a bad impression on e-commerce, which is very much necessary in this present era of the internet. Of the constantly changing international requirements, organizations must implement efficient security safeguards. By all means feasible, they must ensure the prevention of faulty authentication. In the modern-day, cybersecurity is a major worry. There is also a comparison between various phishing tools to ensure that even people apart from experts can be aware of what a phishing attack is and take some measures to prevent themselves from it.

REFERENCES

[1] Sharma, H., Meenakshi, E., Bhatia, S.K. (2017). A comparative analysis and awareness survey of phishing detection tools. In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, pp. 1437-1442. https://doi.org/10.1109/RTEICT.2017.8256835

[2] Mathi, S., Srikanth, L. (2020). A new method for preventing man-in-the-middle attack in IPv6 network mobility. In Advances in Electrical and Computer Technologies: Select Proceedings of ICAECT 2019, Springer Singapore, pp. 211-220. https://doi.org/10.1007/978-981-15-5558-9_21

[3] Alkhalil, Z., Hewage, C., Nawaf, L., Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3: 563060. https://doi.org/10.3389/fcomp.2021.563060

[4] Meena, K., Kanti, T. (2014). A review of exposure and avoidance techniques for phishing attack. International Journal of Computer Applications, 107(5): 27-31.

[5] Akinyelu, A.A., Adewumi, A.O. (2014). Classification of phishing email using random forest machine learning technique. Journal of Applied Mathematics, 2014: 425731. https://doi.org/10.1155/2014/425731

[6] Khonji, M., Iraqi, Y., Jones, A. (2013). Phishing detection: A literature survey. IEEE Communications Surveys & Tutorials, 15(4): 2091-2121. https://doi.org/10.1109/SURV.2013.032213.00009

[7] Patil, P., Devale, P. (2016). A literature survey of phishing attack technique. International Journal of Advanced Research in Computer and Communication Engineering, 5(4): 2091-2121.

[8] Shaikh, A.N., Shabut, A.M., Hossain, M.A. (2016). A literature review on phishing crime, prevention review and investigation of gaps. In 2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA), Chengdu, China, pp. 9-15. https://doi.org/10.1109/SKIMA.2016.7916190

[9] Purkait, S. (2012). Phishing counter measures and their effectiveness–literature review. Information Management & Computer Security, 20(5): 382-420. https://doi.org/10.1108/09685221211286548

[10] Chen, J., Guo, C. (2006). Online detection and prevention of phishing attacks. In 2006 First International Conference on Communications and Networking in China, Beijing, China, pp. 1-7. https://doi.org/10.1109/CHINACOM.2006.344718

[11] Chiew, K.L., Yong, K.S.C., Tan, C.L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. Expert Systems with Applications, 106: 1-20. https://doi.org/10.1016/j.eswa.2018.03.050

[12] Nakkeeran, M., Mathi, S. (2021). A generalized comprehensive security architecture framework for IoT applications against cyber-attacks. In Artificial Intelligence and Technologies: Select Proceedings of ICRTAC-AIT 2020, Singapore: Springer Singapore, pp. 455-471. https://doi.org/10.1007/978-981-16-6448-9_46

[13] Mishra, A.K., Tripathy, A.K., Swain, S. (2018). Analysis and Prevention of Phishing Attacks in Cyber Space. In 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India, pp. 430-434. https://doi.org/10.1109/ICSCCC.2018.8703343

[14] Baykara, M., Gürel, Z.Z. (2018). Detection of phishing attacks. In 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, pp. 1-5. https://doi.org/10.1109/ISDFS.2018.8355389

[15] Zhang, X., Shi, D., Zhang, H., Liu, W., Li, R. (2018). Efficient detection of phishing attacks with hybrid neural networks. In 2018 IEEE 18th International Conference on Communication Technology (ICCT), Chongqing, China, pp. 844-848. https://doi.org/10.1109/ICCT.2018.8600018

[16] Sahoo, P.K. (2018). Data mining a way to solve Phishing Attacks. In 2018 International Conference on Current

Trends towards Converging Technologies (ICCTCT), Coimbatore, India, pp. 1-5. https://doi.org/10.1109/ICCTCT.2018.8550910

[17] Taraka Rama Mokshagna Teja, M., Praveen, K. (2022). Prevention of phishing attacks using QR code safe authentication. In Inventive Computation and Information Technologies: Proceedings of ICICIT 2021, Singapore: Springer Nature Singapore, pp. 361-372. https://doi.org/10.1007/978-981-16-6723-7_27

[18] Athulya, A.A., Praveen, K. (2020). Towards the detection of phishing attacks. In 2020 4th international conference on trends in electronics and informatics (ICOEI)(48184), Tirunelveli, India, pp. 337-343. https://doi.org/10.1109/ICOEI48184.2020.9142967

[19] Kovalluri, S.S., Ashok, A., Singanamala, H. (2018). LSTM based self-defending AI chatbot providing anti-phishing. In Proceedings of the First Workshop on Radical and Experiential Security, pp. 49-56. https://doi.org/10.1145/3203422.3203431

[20] Vazhayil, A., Vinayakumar, R., Soman, K.P. (2018). Comparative study of the detection of malicious URLs using shallow and deep networks. In 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bengaluru, India, pp. 1-6. https://doi.org/10.1109/ICCCNT.2018.8494159

[21] Ulz, T., Pieber, T., Steger, C., Holler, A., Haas, S., Matischek, R. (2018). Automated Authentication Credential Derivation for the Secured Configuration of IoT Devices. In 2018 IEEE 13th International Symposium on Industrial Embedded Systems (SIES), Graz, Austria, pp. 1-8. https://doi.org/10.1109/SIES.2018.8442106

[22] Kuppuswamy, P., Banu, R., Rekha, N. (2017). Preventing and securing data from cyber crime using new authentication method based on block cipher scheme. In 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, Saudi Arabia, pp. 113-117. https://doi.org/10.1109/Anti-Cybercrime.2017.7905274

[23] Salloum, S., Gaber, T., Vadera, S., Sharan, K. (2022). A systematic literature review on phishing email detection using natural language processing techniques. IEEE Access, 10: 65703-65727. https://doi.org/10.1109/ACCESS.2022.3183083

[24] Husák, M., Komárková, J., Bou-Harb, E., Čeleda, P. (2018). Survey of attack projection, prediction, and forecasting in cyber security. IEEE Communications Surveys & Tutorials, 21(1): 640-660. https://doi.org/10.1109/COMST.2018.2871866

[25] Deep, V., Sharma, P. (2018). Analysis and Impact of Cyber Security Threats in India using Mazarbot Case Study. In 2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS), Belgaum, India, pp. 499-503. https://doi.org/10.1109/CTEMS.2018.8769140

[26] https://www.statista.com/statistics/266161/websites-most-affected-by-phishing/, accessed on Oct 2021.

[27] Jeeva, S.C., Rajsingh, E.B. (2016). Intelligent phishing URL detection using association rule mining. Human-centric Computing and Information Sciences, 6(1): 1-19. https://doi.org/10.1186/s13673-016-0064-3

[28] Aburrous, M., Hossain, M.A., Thabatah, F., Dahal, K. (2008). Intelligent phishing website detection system using fuzzy techniques. In 2008 3rd International Conference on Information and Communication Technologies: From Theory to Applicationsm, Damascus, Syria, pp. 1-6. https://doi.org/10.1109/ICTTA.2008.4530019

[29] Fette, I., Sadeh, N., Tomasic, A. (2007). Learning to detect phishing emails. In Proceedings of the 16th international conference on World Wide Web (pp. 649-656). https://doi.org/10.1145/1242572.1242660

[30] Moore, T., Clayton, R. (2007). Examining the impact of website take-down on phishing. In Proceedings of the anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit, pp. 1-13. https://doi.org/10.1145/1299015.1299016