International Journal of Teaching, Learning and Education (IJTLE)
ISSN: 2583-4371
Vol-1, Issue-2, Jul-Aug 2022
Journal Home Page: https://ijtle.com/
Journal DOI: 10.22161/ijtle

Investigating effective phishing attack techniques in cyberattacks using past research

Fatemeh Adel Gholi Kandi, Dr. Roya Mahmoudi, Sahar Ghannadi

Received: 24 Jul 2022; Received in revised form: 15 Aug 2022; Accepted: 21 Aug 2022; Available online: 29Aug 2022

Abstract

The digital world is expanding and evolving rapidly, so cyber criminals attack by illegally using digital assets, especially personal information, to cause damage. Phishing has been one of the biggest concerns as many internet users fall victim to it. Since the first reported phishing attack in 1990, this attack has become a common attack. In the last decade, there have been extensive studies in the field of phishing attacks. This research examines how phishing attacks and methods to prevent such cyber-attacks have been done to identify the process of preventing and detecting these attacks in the future. This review article has been conducted to review academic literature and research conducted on phishing attacks to learn about these attacks and how to counter them. The review of articles and research from 2018 to 2022 will be presented using content analysis in a general and understood framework of phishing attacks.

***Keywords*— Phishing attack, cyber-attack, theft, email, security, confidential information, victim**

I. INTRODUCTION

The development of information technology brings many benefits to people and businesses, but at the same time, information technology acts as a gateway for criminal activities. One of the most threatening crimes of all internet users is "identity theft", which is called phishing. A phishing attack is a cyberattack that aims to defraud and obtain confidential information from the targets. A phishing attack may use different communication channels and the most common ones are email messages, phone calls, messages on social networks, and others. Identifying phishing messages is critical to combating phishing and reducing leading cybercrimes. While technical anti-phishing solutions are not accurate enough, training and understanding the phishing attack landscape are critical to ensuring personal and organizational security. Phishing has been claimed as one of the biggest attack vectors that cause a lot of damage to online services and data security. This cybersecurity threat is an attempt to trick Internet users into revealing their personal information, such as passwords or financial account credentials. Usually to steal in the form of an email (spoof email) or impersonate a legitimate website, so that the victim cannot distinguish between phishing and legitimate web pages. Additionally, the attacker can use key phrases to emphasize a sense of urgency to the victim, for example, "You must complete this account review now." Based on data reported by Verizon, (Ansett, 2021), it was noted that 30% of phishing emails were read by victims (Cranover, 2018). It was also reported that 12% of those victims clicked on fake websites or fake attachments (Chen et al., 2018). The purpose of this article is to express the appropriate techniques to prevent phishing attacks in different ways and raise the level of awareness of users to detect phishing attacks so that users do not suffer irreparable damage. This article, it is explained how phishing attacks appear and how to recognize these attacks and how to prevent such attacks. Several techniques are presented to counter these phishing attacks. In the next section, the steps of conducting the research, how to access the articles, and the selection criteria will be explained, and with what keywords were used to access the research and from

which database these items were accessed. In the third part, it will be done by examining the research done on different dimensions of phishing attacks and extracting key points from each article, and comparing their performance in the last part, will be concluded by discussing the output of the results and the specifics and issues of future research.

II. METHOD OF DOING WORK

Due to the importance of the topic of phishing attacks in recent years and many types of research have been done, in this article, we have tried to analyze the content of some of the most recent research conducted from 2018 to 2022 and collected the report on the performance of each in a specific part of phishing attacks. Elsevier, Science Direct, ISI Web of Knowledge, Google Scholar Scopus, Springer, and IEEE databases were used to search for research which was searched by using the main keyword of phishing attacks and sub-keywords of cyber, e-mail, and website. 40 articles in this field were collected and it was checked that 15 articles were fully reviewed and the rest were discarded due to their ineffectiveness. This number was selected according to the reference of each of the articles to the key topics of phishing attacks and the most recent dates for the continuous change of technology and approaches. In the next section, the review of the selected articles is discussed.

Table 1- reviewed articles

Title	Name of the author/authors	year of publication	The title of the journal or conference
Detection of phishing attacks	Muhammet Baykara * Zahit Ziya Güre	2018	IEEE
Phishing Attacks: A Recent Comprehensive Study and a New Anatomy	Zainab Alkhalil *Chaminda Hewag	2021	Frontiers in Computer Science
A Novel Approach to Detect Phishing Attacks using Binary Visualisation and Machine Learning	Luke Barlow	2020	IEEE
Machine Learning Mechanisms for Cyber-Phishing Attack	Yu-Hung CHEN	2019	The Institute of Electronics, Information and Communication Engineers
Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender on Thai Employees Associated with Phishing Attacks	Therdpong Daengsi	2022	Education and Information Technologie
Improving cybersecurity awareness using phishing attack simulation	Surachai Chatchalermpun	2020	Conference on Computer Science and Engineering Technology
E-mail-Based Phishing Attack Taxonomy	Justinas Rastenis	2020	Applied sciences
Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process	Hossein Abroshan* Geert Poels	2021	IEEE

Cross Ref DOI: 10.22161/ijtle.1.2.4

Types of anti-phishing solutions for a phishing attack	Siti Hawa Apandi &	2020	IOP Conference Series: Materials Science and Engineering
Detecting the Phishing Attack Using Collaborative Approach and Secure Login through Dynamic Virtual Passwords	Robbi Rahim	2020	Webology

III. FINDINGS

3.1 Research reviewed

First reference: Phishing is a type of cyberattack that is defined as the fraudulent acquisition of confidential data by intended recipients and the misuse of this data. An example of phishing; The email is from a known website from the user's bank, credit card company, email, or internet service provider. Phishing is often used to obtain personal passwords or credit card information. We use an "anti-phishing simulator" thanks to a database connection and classification algorithm that decides whether a message is phishing or not. In this way, you can check whether the links on the page are valid or not. Anti-Phishing Simulator aims to control information security and prevent violations, it allows the user to check whether spam is present in the current database or not.

Second reference: In phishing attacks, phishers use social engineering techniques to direct users to malicious websites after receiving an email and following a defined link (Guptav et al, 2015). On the other hand, attackers can abuse other things such as Voice over IP (VoIP), short message service (SMS), and instant message (IM) (Gupta et al. 2015) A technique called spear-phishing is used by cybercriminals, usually from users with a lack of technical skills, poorly trained and more vulnerable users to achieve their goals, for example, emails that offer great discounts or gifts, cards and Others (Workman, 2008) nearly 90% of organizations faced targeted phishing attacks. Of those, 88% experienced spear-phishing attacks, 83% voice phishing (vishing), 86% dealt with social media, 84% reported SMS/text phishing attacks (SMishing), and 81% reported malicious USB drops.

Third reference: Another new method of detecting phishing in cyberattacks is leverage In the case of multi-level artificial intelligence, a combination of neural networks coupled with binary visualization using visual representation techniques allows us to gain insight into the structural differences between legitimate and phishing webs And capable of quickly identifying the phishing attacker with high accuracy, this technique consists of two stages, the learning stage, and the detection stage. Web scraping automation protects users from visiting potential phishing pages and eliminates the risk of drop-ins and browser abuse. When the website source code is scraped and saved, the corresponding binary file is sent to the image generation module, where the Binvis image visualization method is used to convert the binary files into 2D images. Tensor Flow neural networks are analyzed to perform classification. This can greatly minimize the time and space of phishing website classification.

Fourth reference: Phishing attacks in cyberattacks, From the blacklist, are mainly used to detect phishing. The blacklisting method is mainly based on acomparison with phishing links previously reported by victims. However, this technology has some problems, once the URL is successfully matched with the URL in the database, it is identified as a suspicious or dangerous URL and the user is warned and blocked. To ensure that the user can identify it and protect themselves, the number of phishing sites is generally significantly higher than the number of legitimate sites, because hackers usually use a site, for example, https://192.168 .0.159/index.php is used. Therefore, well-known domain names are often added as subdomains to phishing URLs, which can be used to confuse victims into believing that the URL is a legitimate website. They usually add special symbols like @, —, *, to the URL, mainly to confuse the user. and thereby allowing the user to click on a phishing link. When the extracted feature URL is sent to the feature evaluation algorithm for analysis, the feature information and irrelevant noise are filtered out. There are three bases for evaluation, which are the evaluation of the degree of data clustering, data distribution, and data independence. After the feature evaluation, the time of the extracted final feature can be greatly shortened.

Fifth reference: Gender and age affect cyber security awareness, a spear-phishing attack was simulated at a

Cross Ref DOI: 10.22161/ijtle.1.2.4

large financial services organization in Thailand with 5,885 male and 14,279 female employees, and the first stage of the phishing simulation was that 23.4% of Employees opened malicious emails. While 22.1% of them not only opened the email but also clicked on a link, it means they had little awareness of cyber security. However, after presenting an approach, which was based on the transfer of knowledge developed from guidelines and frameworks related to cyber security, it was found that the cyber security awareness of employees improved significantly Because, after ,that intervention, 94% of them improved Gender plays a role in cyber security awareness Thai female employees in a financial services company had a higher level of cyber security awareness than male employees.

Sixth reference: Cyber exercises and cyber security knowledge transfer can improve the level of awareness of cyber security in financial institutions A targeted section for attackers. Therefore, by raising the level of awareness among all workers, it can help reduce risks or threats, and it is also more likely that a potential victim will report a suspicious incident and an appropriate incident response will be made in time to reduce harm. The methodology of phishing emails includes three security approaches 1. Phishing simulation using phishing emails 2. Knowledge transfer 3. Security awareness

This experiment was conducted in 2 stages in Thailand in a large organization. In the first stage, an email was sent and the email fully explained phishing attacks, but some users opened the email. The second stage, the phishing simulation was done again in 2020. The content of the email was related to an advertisement from a popular e-commerce website in Thailand called "Shoppee" The second phishing email with fake ads was sent to the same targeted users as in the first stage. Results: Phase 1: A phishing email with Gmail storage space was sent to about 20,340 workers. After answering those users, all the received answers are divided into 4 categories76.75% took no action, while 23.25% of users opened the email 6.93% opened the email and just clicked on the link and 15% opened the email, clicked on the link and filled it out. The results of the second stage, which was carried out after the knowledge transfer, spear-phishing email by sending Shoppe ads to about 20,260 users. After they responded, all responses were 93.24% took no action, while 6.76% of users opened the email. In this section, it was found that 0.85% only opened the email, 3.85% opened the email and only clicked on the link, and 2.06% opened the email, clicked on the link, and filled in their password. Comparing the data of the second stage and the first stage, focusing on the part of workers classified as possible victims, the percentage of responses of these users has decreased by about 16.5%.16% just for opening the email, opening and clicking on the link, and 13% click to open the email, respectively, the link and password are filled.

Seventh reference: Email-based phishing attack classification consists of six items, attack stages, each stage has at least one criterion for attack classification. Using classification to flag phishing attacks increases awareness A phishing attack may use different communication channels, the most common of which are email messages, phone calls, messages on social networks, etc. Classification is one of the most widely used approaches to represent the subject of cybercrimes and providing taxonomy will enhance the proper understanding and understanding of the overview.

A phishing attack consists of six steps based on email:

1. Email address selection: To execute an email-based phishing attack, an email address or the address of a potential victim must be obtained. At this stage, different strategies are used for email address selection. Therefore, we divide the stage of address selection with various strategies.
2. Creating email content: The content and text of the email for the phishing attack must be ready for the victim to participate in the phishing attack, this step is very important and it can be classified based on multiple criteria.
3. Sending an email to recipients: The way the attacker sends the email to the phishing victims is an important factor, in the phishing attack strategy chosen by sending phishing emails; Therefore, we describe the step of sending an email based on three parts: using the sender's email address; the number of recipients in the phishing attack; Using the phishing attack strategy, the possible classes for each of the criteria are presented in the classification.
4. Waiting for a response from email recipients in most cases, the attacker just waits for the victim to respond to the phishing email. However, in the case of a systematic strategy of a phishing attack, some additional measures can be implemented while waiting for the victim's response. The possible categorization of the attacker's actions while waiting for the victim's

Cross Ref DOI: 10.22161/ijtle.1.2.4

response is part of a systematic email-sending strategy.

5. The results of phishing attacks and data collection, the main goal of a phishing attack is to receive some specific data from the victims. Also, we classify the types of data collected into possible classes for these criteria.
6. Use of results and collected data So we make a list of possible targets that the attacker may have using the data collected by phishing attacks.

The obtained results of an email-based phishing attack classification are presented as a tree structure that defines the steps of an email-based phishing attack in the classification, each stage has at least one criterion for the details of the phishing attack, and email-based phishing attack classification has a wider range of classification criteria.

Eighth reference: The level of risk-taking and decision-making styles of people affect the probability of becoming a victim of phishing. Users with a phishing attack can affect their risk-taking on behavior and ethics. Cybercriminals use cognitive and behavioral aspects of humans to design phishing attacks and deceive victims by doing two characteristics of risk-taking behavior and decision-making style, both of which can play a role in making people fall into phishing traps. in the first step, the phishing message is designed to look genuine and by using the same format as the real organization including their logo, the fraudsters use various techniques to convince the user to open an infected attachment or Click on the link. as a result, fraudsters try to gain the victim's trust and encourage them to click on a link to open a phishing email (an infected attachment) and eventually share sensitive information on a phishing website, such as account details. banking or confidential information about their organization. Research findings have implications for security management in organizations. For example, assessing the risk-taking behavior of an organization's employees and adapting company policy to include specific security and anti-phishing training opportunities (especially for high-risk users) There are two ways to help prevent successful phishing attacks and the resulting risks. There is no significant effect of the mentioned psychological risk-related behaviors and decision-making in sending information on phishing websites.

Ninth Reference: To solve a phishing attack, anti-phishing solutions are needed. Phishing attack approaches can be divided into two categories, which include social engineering and malware-based phishing attacks. Social engineering is the most sensitive thing a user has that phisher attacks to exploit, so the user reveals their personal information to the phisher. For Malware - Based on a phishing attack, it secretly installs malicious programs to allow the phisher access to the user's computer. There are two types of anti-phishing solutions, which are phishing prevention and phishing detection. Detecting phishing can be divided into two categories, which include user awareness and software detection. User awareness is about educating users so they can identify phishing attempts that target them. Users should be careful to check the URL of the web page first when visiting a web page, for example, even if the user is careful, there is a possibility that the user can be tricked by a phisher into visiting a phishing web page. Therefore, software detection is introduced for website legitimacy or software detection phishing can be divided into two traditional methods and the automatic method, and for the traditional software detection method, the black list is used to manage the phishing list Websites that are manually entered and updated in the system. The advantage of the blacklist is that it has high accuracy, the disadvantage of the blacklist is that it does not identify the phishing website, which is short-lived. The automatic software detection method uses a combination of heuristics and blacklisting. The heuristic-based approach examines the contents of the website. There are three types of exploratory approaches based on surface content, textual content, and visual content. The surface content heuristic means checking the website address, the textual content heuristic means checking terms or words on the website, and finally heuristic visual content means checking the website design. Next, we use the general phishing detection toolbar and academic phishing detection/classification schemes, the purpose of the general phishing detection toolbar is to identify and block phishing websites. The user can see this toolbar as a web browser extension and a security warning will be displayed. The phishing toolbar is a useful tool to protect Internet users who do not have enough knowledge to identify a phishing attack. To detect general phishing in the toolbar, it is difficult to know the algorithm used to detect phishing The goal of academic phishing detection/classification schemes is to identify and classify whether a website is legitimate or phishing. It uses artificial intelligence (AI) under the supervision of classification algorithms. Algorithms used for phishing detection techniques are Support Vector Machine and Logistic, and there are two types of anti-phishing solutions to solve phishing attacks. Phishing Prevention

Cross Ref DOI: 10.22161/ijtle.1.2.4

and Phishing Detection Before we can perform phishing, we must first perform phishing detection. If a phishing attack is not detected first, there is no point in preventing phishing. Once a phishing attack is identified, only then can phishing prevention be implemented Common phishing detection toolbars and academic phishing detection/classification schemes are useful for identifying phishing attacks.

tenth reference: Protecting user information is a big problem in the technical world. To protect against phishing attacks, they use the technique of virtual passwords to log in so that users can protect their usernames and passwords against keyloggers, malicious bots, or spyware This technique has a virtual keyboard that is generated after each time the user uses the website When clicked, the keyboard changes its position, and the position of the keys is hidden so it is difficult to identify those keys pressed by the user. Using a virtual keyboard to capture authentication details is safer for users and makes it harder for malware to identify one of the main problems with passwords when a user logs into a website. which is widely used, a variety of equipment and tools, for example, BackTrack and Cain, which help hackers to decrypt and identify HTTPS programmers use this model for authentication, researchers found that this model is easy to make and completely safe.

3.2 Comparison of the conducted research

In this section, the advantages and disadvantages of each article are discussed in the form of Table 2.

Table 2- Comparison of the reviewed research works

Title	Advantages	Disadvantages
Detection of phishing attacks	In the classification algorithm, they do not need prior knowledge of the problem and can detect malicious emails	This module allows the user to mark spam as spam. Every spam may not be spam.
Phishing Attacks: A Recent Comprehensive Study and a New Anatomy	3 important features of raising the level of users, how to detect and how to deal with the attack	It was a general study, but the psychological effects of phishing attacks on users were not discussed
A Novel Approach to Detect Phishing Attacks using Binary Visualisation and Machine Learning	Faster time and high accuracy to detect aphishing site	The article has developed a qualitative approach
Machine Learning Mechanisms for Cyber-Phishing Attack	Using a blacklist to prevent cyber attacks	Lack of reliability
Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender on Thai Employees Associated with Phishing Attacks	Examining awareness factors with new techniques has been tested on users	The samples were for a specific region and may not have been comprehensive in other regions
Improving cybersecurity awareness using phishing attack simulation	Cyber training can improve user awareness	Users can identify Not every indicator in every email is phishing
E-mail-Based Phishing Attack Taxonomy	Attacks are classified into 4 categories	There is no single format for classifying phishing
Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process	A comprehensive framework consistent with risk-taking behavior and decision-making style	Failure to provide a model to prevent attacks

Cross Ref DOI: 10.22161/ijtle.1.2.4

Types of anti-phishing solutions for aphishing attack	Creating public and academic phishing detection toolbars detection/classification schemes for users with a low level of awareness	It is a qualitative approach and tests for hypotheses have not been done.
Detecting the Phishing Attack Using Collaborative Approach and Secure Login through Dynamic Virtual Passwords	System analysis for security, speed, and ease of use	The main problem of identifying the password when the user enters the Internet

In all reviewed articles, the aspect of protecting personal information, credit cards, is considered to be the first priority for creating techniques for phishing attacks. Protecting privacy against phishers is very important. For example, when a malicious email is sent to a person, have full awareness and ability to identify such attacks, which includes raising awareness, using anti-phishing software and anti-phishing techniques. In terms of raising the level of awareness, more people will be able to identify such attacks, and in terms of software, there is software that has artificial intelligence and is able to detect phishing attacks in various other sectors, which helps protect privacy against phishing as we know, phishing attacks can cause irreparable damage to individuals and large organizations, that's why this issue is so important. We can prevent it by raising the level of awareness and using new techniques against phishers who use new techniques every day to trap their users.

IV. CONCLUSION AND FUTURE RESEARCH

Analyzing the content of the studied articles and examining the key concepts and methods and structures of research and the achievements of each article, we were able to name a few techniques to prevent phishing attacks by using the analyzes carried out and how to get familiar with phishing attacks and with what malicious intent phishers carry out these attacks and how phishers attack, research has brought many advantages. For example, it has been able to introduce new techniques to prevent phishing attacks, and by raising the level of awareness, such attacks can be prevented or pre-empted and have a direct and positive impact on users in using security methods in this article, the most important features of phishing detection methods are mentioned in a sequel to the article, the behavior, and motivation of opening malicious emails are researched and People with a high-risk tolerance have a high percentage of clicks on malicious emails. Users can identify and prevent malicious attacks by raising awareness and reducing the opening percentage of malicious emails to a low percentage also, following that, women and men, age ,groups and education can be effective in detecting attacks and opening malicious emails. A general model focuses on phishing attacks and defines how we can protect against these attacks and how we can detect them. Past research emphasizes some factors as key factors, but due to the increasing growth of phishing attacks and the impact of these attacks on people's lives, these factors should be revised it should be investigated in the section on cyberattacks. For this purpose, it is suggested that the effective factors in successful and definitive prevention should be investigated qualitatively and quantitatively in future research.

REFERENCES

[1] Baykara, M., & Gürel, Z. Z. (2018, March). Detection of phishing attacks. In 2018 6th International Symposium on Digital Forensic and Security (ISDFS) (pp. 1-5). IEEE.

[2] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and new anatomy. Frontiers in Computer Science, 3, 563060.

[3] Barlow, L., Bendiab, G., Shiaeles, S., & Savage, N. (2020, October). A novel approach to detect phishing attacks using binary visualization and machine learning. In 2020 IEEE World Congress on Services (SERVICES) (pp. 177-182). IEEE.

[4] CHEN, Y. (2019). Machine Learning Mechanisms for Cyber-Phishing Attack. IEICE TRANS. INF. & SYST.

[5] Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2022). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. Education and Information Technologies, 27(4), 4729-4752.

[6] Chatchalermpun, S., & Daengsi, T. (2021, February). Improving cybersecurity awareness using phishing attack simulation. In IOP Conference Series: Materials Science and Engineering (Vol. 1088, No. 1, p. 012015). IOP Publishing.

[7] Rastenis, J., Ramanauskaitė, S., Janulevičius, J., Čenys, A., Slotkienė, A., & Pakrijauskas, K. (2020). E-mail-based

phishing attack taxonomy. Applied Sciences, 10(7), 2363.

[8] Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing happens beyond technology: the effects of human behaviors and demographics on each step of a phishing process. IEEE Access, 9, 44928-44949.

[9] Apandi, S. H., Sallim, J., & Sidek, R. M. (2020, February). Types of anti-phishing solutions for a phishing attack. In IOP Conference Series: Materials Science and Engineering (Vol. 769, No. 1, p. 012072). IOP Publishing.

[10] Rahim, R., Murugan, S., Mostafa, R. R., Dubey, A. K., Regin, R., Kulkarni, V., & Dhanalakshmi, K. S. (2020). Detecting the Phishing Attack Using Collaborative e Approach and Secure Login through Dynamic Virtual Passwords. Webology, 17(2).