Journal of Information and Knowledge Management (JIKM) Vol 1 Special Issue (2022)

A Theoretical Framework for The Awareness of Phishing Attack

Aida Rozihan Mohamad Asri and Irni Eliana Khairuddin

School of Information Science,
College of Computing, Informatics and Media
UiTM Selangor Branch, Puncak Perdana Campus, 40150 Shah Alam, Selangor, Malaysia

Email: aidarozihan@gmail.com

Received Date: 30 August 2022
Accepted Date: 21 September 2022
Published Date: 1 November 2022

Abstract. The increasing of internet usage as well as rapid technology evolves has caused the growing number of people who commit to cybercrime. Phishing is a type of cyber-attack in which an attacker sends a message to a targeted individual or organization with the intent of stealing personal information that phishers can use against them. Since phishing attacks are being developed and rising every year, internet users need to educate themselves and gain some knowledge about phishing attacks. The objective of this paper is to discuss the awareness of people towards phishing attack

Keywords: Phishing attack, threat, cybersecurity, fraud, information management, information management

1 Introduction

As the digital footprint of Internet users grows to include social networks, financial information, and data saved in the cloud, the security of this entire identity is frequently underpinned by a single account, an email address. This foundation of trust is undermined because of the disclosure of a victim's email password or recovery questions. Once a victim's account has been compromised, a hijacker can reset the victim's passwords to other services as a steppingstone attack; download all of the victim's private data; remotely wipe the victim's data and backups; or impersonate the victim in order to send spam or other harmful communications. Since the number of people who use the internet grows, and the technological evolution moves fast, so does the number of people who commit cybercrimes. Cyber fraud has become a severe problem in many parts of the globe (Kamruzzaman, Islam, Islam, Hossain, & Hakim, 2016). There are many types of cyber fraud, like Phishing, scamming, hacking and stealing information from people's computers. People have not thought about

how others can see their data because they rely on the internet. This makes it easy for cybercriminals to get victims. People have become unaware to the transparency of their information due to their reliance on the internet. Because of this, cybercriminals can easily trap victims. In addition, cybercriminals use human psychology, also known as social engineering, to deceive their victims. According to Krombholz, Hobel, Huber, and Weippl (2014), social engineering is the human psychology used to manipulate individuals into providing confidential or personal information for fraudulent purposes. Human psychology is one of the reasons why society is vulnerable to phishing attacks. This is because, phishing is a technique used to get personal information to commit identity theft. Phishing has been proven to be the most successful of all cyber-attacks and is the most often used attack vector. Attackers typically do this by using forged email messages, URLs, and websites. Now, users face a new threat from online access and social media. In this brief paper, we discuss the stages of a phishing attack, the type of phishing attack, the phishing attack technique, and phishing attack prevention. The objective of this paper is to raise people's awareness of phishing attacks so that they can be informed about the impact and severity of phishing attacks on people and organisations so that they can take appropriate action.

2 Literature Review

Nowadays, the internet is a dangerous place to be. Hackers are continuously targeting users' personal information and passwords. Even though most websites on the internet are secure, this cannot be said for all of them. In order to acquire unauthorized access to sensitive information, these rule-breakers do not follow the rules at all and instead rely on fraud and hacking. (Bhuvana, Bhat, A. S., Shetty, T., & Naik, M. P. 2021). Phishing is a type of cyber-attack in which an attacker sends a message to a targeted individual or organization with the intent of stealing personal information that phishers can use against them. The Phisher and Intruder can steal data in a variety of methods in order to get what they want. As a result, Internet users must be cautious while accessing any website or clicking on any URL. Even though numerous software, approaches, and tools are available, such as spam filters and antivirus software, we should be cautious of phishing attacks. (N. Singh, L. Thrushitha, J.M.Reddy, 2021). Additionally, Phishing is a deceptive attempt to gain sensitive information such as usernames, passwords, online banking, and credit card information. (Katkuri, 2018) The objective may be to steal their money, obtain critical information, or even download malware and unintentionally manipulate them. This is because malware is essentially spam email. Spam can be considered non-intrusive propaganda sent by unsolicited emails, SMS texts, or social media communications. Spam may contain viruses or malware intended to exploit the receivers' personal or sensitive information. (Talos, 2018). According to statistics, phishing emails account for more than 50% of global email traffic, 15% of unique users and 85% of organizations have faced a phishing attempt at least once. (Suryavanshi, Nirmala, and A. Jain, 2016).

2.1 Stages of Phishing Attack

Phishing attacks are dangerous not because of technical flaws but because of human gullibility and inattention. Often, phishing attacks rely on social engineering, which exploits human fallibility rather than physical weakness. A phishing attack begins with the cybercriminal gathering information about the target, then utilizing that data to generate a link and convincing the victim to take action. A typical phishing attempt consists of three stages: bait, hook, and catch.(M. Khonji, Y. Iraqi, and A. Jones, 2013)

2.1.1. Bait

The bait is frequently an email message purporting to be from a credible person or organization, whose credibility is bolstered by curiosity, such as emails with compromised links that appear to connect to videos of recent news or exciting events. (K.D.Tandale &S.N.Pawar, 2020). It is natural to be scared when a 'bank' email pushes customers to authenticate their information in light of account breaches. Also, the phisher will try to bait the victim by impersonating bank officials and promoting packages with higher interest rates to attract customers in such scenarios and make users make cash transfers to newly created accounts in the attacker's web trap. (S.Patil & S.Dhag, 2019) Additionally, the phisher will send an email imitating a friend or family needing financial aid, and they will believe it.

2.1.2. Hook

After acquiring the vital information to serve as bait, the attacker must start to set the hook. The hook in many scams includes convincing the victim that one of their accounts has been hacked, instilling a sense of urgency, and pushing the target to take fast action, possibly without thinking. (A.A. Andryukhin, 2019). To genuinely persuade the victim to act, the attacker must offer a promise or terrify them into action. The attacker can now lead the victim to click on a link that takes them to a page to collect the victim's information.

2.1.3. Catch

Phishing's third step is the actual attack. The cybercriminal sends the email and waits for the target to click. What the attacker does next is determined by the nature of the fraud. For instance, imagine they accessed the victim's email password via a landing page. Then they can access the victim's email account to obtain further information and begin sending other phishing emails to the victim's contacts. (P. Liu and T. S. Moh, 2016).

2.2 Type of Phishing Attacks

A phishing attack proceeds in three stages. The first is to deliver a phish to a victim. The second is to notify the victim to take action specified in the message, often visiting a website or downloading malware. The third is to sell stolen data

illegally. Typically, this phishing email uses social engineering techniques rather than technical ones to fool victims. (K.D.Tandale &S.N.Pawar, 2020). Based on a research paper by A.A. Andryukhin (2019). Phishing attacks can be divided into two types which are social engineering schemes and technical schemes.

2.2.1. Social engineering schemes

Social engineering schemes rely on deceit and the victim's subsequent individual harmful acts. Social engineering can trick those unfamiliar with these sorts of attacks. In addition, they can also embed malicious viruses, Trojan, and other dangerous malware. (A.A. Andryukhin, 2019). The attack is launched by sending misleading information to users. It is activated when they do particular actions such as opening the mail, clicking on the link, or downloading the malicious file. According to the previous research paper, whenever a user clicks on any suspicious link they receive through any platform, just one click is sufficient to gain the victim's personal information. (Boateng & Amanor, 2014).

2.2.2. Technical engineering schemes

Technical engineering schemes exploit software and infrastructure weaknesses and imperfections because this attack is more labour-intensive but less noticeable than social engineering schemes. The percentage of goals achieved in Phishing is significantly more significant than in the social engineering scheme. This scheme uses the session hijacking technique, such as cookies hijacking. (Gupta, Singhal, & Kapoor, 2016). The attack is predicated on using a legitimate computer session, occasionally a session key, to obtain unauthorized access to data or services on a computer system. It is used specifically to refer to stealing a cookie used to authenticate a user on a remote server. A common technique used is source-routed I.P. packets.

2.3 Type of Phishing Attack Technique

Generally, phishing attacks can be carried out in various ways, depending on the phisher's capability. They have designed some attacking strategies. The following are several popular phishing techniques among internet users: deceptive Phishing, spear phishing, malware-based Phishing and social media Phishing. (N. Singh, L.Thrushitha, J.M. Reddy, 2021). In addition, with the development of do-it-yourself kits for Phishing, almost anybody wants to become a phisher without knowing what disaster is coming to them later. According to Himani Thakur & Dr Supreet Kaur (2019), Deceptive Phishing is similar to the instant spam messages technique. It also uses messages to obtain the user's bank account details and personal data. In addition, those emails use threats and a sense of urgency to scare users into doing what the attackers want by using legitimate links for this phishing attack. The attacker avoids detection by email filters by including actual links in their fraudulent phishing emails. They might accomplish this by providing contact information for a mock organization. Other than that, the technique of Redirects and shortened links always can fool the victim of phishing attacks because malicious actors do not want to raise any red flags with their victims. They, therefore, use shortened URLs to cheat Secure Email Gateways (SEGs). They also use "time bombs" to redirect users to a phishing

landing page only after the delivered email. After victims have forfeited their credentials, the operation redirects victims to a legitimate web page.

The term "spear-phishing" refers to an email or electronic communication fraud that targets a single individual, company, or organization. In addition to stealing data, cybercriminals may seek to install malware on a targeted user's electronic devices. (D.Kempe,Walrave, Hardyns, Pauwels & Ponnet, 2018). According to Christopher Shaw (2020), this attack is much more deliberate to enhance the potential to succeed. It primarily targets each individual's social media accounts and other personal information. These attackers want more critical information than just credit card numbers. Here are some of the most common techniques used in spear-phishing attacks. One of the spear-phishing techniques is to host harmful documents on cloud services. Malicious documents are stored on cloud services such as Dropbox and Google Drive. Next is through exploring the victim's social media. An evil criminal must ascertain who is employed at the targeted organization. They can accomplish this by utilizing social media platforms such as LinkedIn to investigate the organization's structure and decide their targeted attacks. Other than that, Malware-based Phishing is a technique with a high probability of installing and running faulty software or harmful code on the victim's computer or personal device. This malicious code connects all of the victim's emails related to financial transactions. When a victim clicks on a malicious link inadvertently, the malicious link obtains all of the user's online account information. Malware-based Phishing primarily targets small and medium-sized enterprises that do not update their software packages regularly. (G. J. W. Kathrine, P. M. Praise, A. A. Rose & E. C. Kalaivani, 2019).

Social media phishing is the most common phishing attack. Attackers use Facebook, Twitter, LinkedIn, and Instagram to steal personal information or trick victims into clicking on malicious links promising a job or reward. Phishers may use the victim's familiar name to create fake accounts. Phishers may create false accounts using the victim's name to fool them. Phishing is common on social media. The attacker creates a bogus website that looks real to deceive victims. Phishing attacks are often used to steal user data. The phisher forged "sign-in" emails. As a result, the user clicks on the link, allowing the attacker to steal their data. That is why social media users should be aware of social media phishing and try to learn about these issues that might happen in the future.

2.4 Prevention of Phishing Attacks

According to F. Mouton, M. Malan, L. Leenen, and H.S. Venter (2019), Phishing is a significant issue in the internet's ever-expanding service. There are several techniques to trick someone into providing personal information using social engineering techniques. Phishing can be described as the combining of technology and social engineering. Whereas phishing attacks can be successful in a situation where one of these components dominates over the other, it is likely to be the case that the success rate would increase when the attacker uses both of these components strategically. This means that in preventing phishing attempts, one should understand both parts. (M. Jakobsson, 2018). There are four (4) ways to avoid phishing attacks. Firstly, attackers come from people who are not recognized. They will ask for confirmation of personal or financial information over the internet and for the

information to be given to them. (V. Bhavsar, A. Kadlak & S. Sharma, 2018). Second, people can only get in touch with each other over the phone or through safe websites. During online transactions, the user should look for the "HTTPS" URL, which has the "s." instead of "HTTP," to show that the site is safe and not a scam. (V. Bhavsar, A. Kadlak & S. Sharma, 2018). Third, do not click on links, download files, or open attachments in emails from an unknown sender**.** Protecting critical information, like your bank account number or social media account information, is always best. In emails, only open attachments when you know what they are and expect them, even if you are the sender. (V. Bhavsar, A. Kadlak & S. Sharma, 2018) . Fourth, security awareness training, if you work for a company, educate and demonstrate to staff what a good email should look like. Manage and teach employees how to recognize and avoid phishing attacks. Finally, training users will help limit the success of assaults, while testing will ensure that security and management are prepared to respond appropriately. (V. Bhavsar, A. Kadlak, and S. Sharma,2018).

3 Discussion

Social engineering has become the most dangerous technique that has been use by the fraudster and the cybercriminal. According to Kennedy and Parsons (2012, 2014), Atkins and Huang (2013), Krombholz et al. (2014), Kamruzzaman et al. (2016), Muniandy et al. (2016), and Parsons et al. (2019), social engineering has a negative effect on phishing awareness. Ferreira and Telesa (2019), stated that social engineering has a few persuasive principles. The first principle is authority, where the fraudsters would pose as representatives of reputable organizations. Society teaches us to follow the norms in our social interactions and never to question or criticize authority. This circumstance provides the opportunity to pose as an authority for the con artists. They are terrified after getting calls or messages from the authorities even if they know society would heed them. Social proof is the second principle. People frequently adopt a specific behavior in each setting by imitating the acts of others. Fraudsters use this chance to persuade their victims that they are not alone in their actions and that others are engaging in similar behavior. Similarity and deceit make up the third social engineering persuasion principle.This idea relates to how people connect in real life when they search for more agreeable and comparable characteristics in them. Unless they have reason to suppose something is amiss or a particular behavior is completely unexpected or manipulative, people prefer to believe what others say or do. Distraction is the fourth persuasion strategy in social engineering. This circumstance arises when there are some limitations or a finite amount of time for the products being offered, and people are intensely focused on gains, losses, or wants. People would often have fewer factors to evaluate carefully before making decisions. The thieves would steal the victims' money because they knew their financial information. In addition, Lawson, Pearson, Crowson, and Mayhorn (2020) used the example of fraudsters using a sense of urgency to divert victims by stating that the management would cancel the account in the following 24 hours. Other than that, People are urged to be vigilant against the influence of social engineering by constantly remaining up-to-date on phishing techniques and anti-phishing expertise by reading other phishing materials. They should also protect their data with concrete password credentials and anti-virus

software. This study is valuable to society's understanding and comprehension of phishing. In addition, industries and government organizations can use the findings of this study to raise employee knowledge and implement appropriate countermeasures against phishing attacks.

4 A Proposed Framework for Assessing the Phishing Attack Severity and Susceptibility

Although phishing attacks are common in a technological society, people still get tricked by the attackers, which could lead them to misery. Not everyone thinks about the consequences of being tricked until they feel it for themselves. When data travels through physical connections, not everyone is aware of the risks of cyber-attacks on the internet. Students in schools or universities sometimes do not consider the internet's risks. They might be excited about using social media, sending and receiving emails, and downloading or uploading files. However, they might not know the cyber security risks of doing these things. There are a lot of potential risks that the students do not realize. (H. Mary & C. Elenita, 2019). Also, it is hard to find phishing attacks with high accuracy because they are a type of attack in which users are tricked by phishers who use social engineering methods to steal their private or personal information for their benefit. (P.K. Sahoo, 2018). This is especially true if someone sends a fake email that looks like it came from a well-known brand or organization and asks for personal information like bank passwords, usernames, phone numbers, and so on. Regarding to the previous studies, It has been confirmed by the Anti-Phishing Working Group (APWG) that the number of phishing attacks has increased to 1,220,523 cases since 2016, making it the highest number reached since 2004.

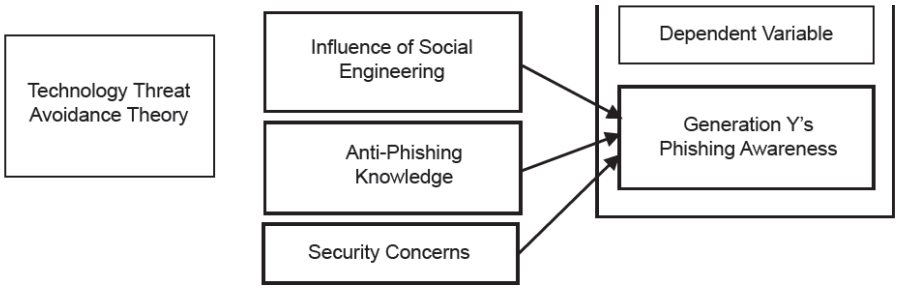

Figure 1: Technology Threat Avoidance Theory Framework (Source: Farhana, Zaharon and Ali, 2021)

It is abundantly clear that phishing attacks are the most dangerous form of online threat in the entire world. (Rao&Pais, 2019). The evaluation methodologies and metrics for phishing attacks differ according to whether they are seen in the technology development, such as new technology threats, awareness, or solutions for the problems. The criteria of phishing attack research evaluation are based on their functional, prevention, use assessment, and ethnographic study. They are comprehensive but concise in that they cover the whole spectrum of essential

outcomes while maintaining a systematic and manageable evaluation framework with no redundancies. The evaluation must be accurate and unambiguous, which means a direct and accurate link between the criteria and their actual outcomes. Each of the four categories of usability evaluation criteria is separated into a subcategory: content, procedure, format, and overall evaluation (of the usability). When it comes to using criteria, the evaluation process is often centred on usage patterns; material usage; usage statistics; and who, what, when, and for what reasons to evaluate the phishing attack research criteria.

The theoretical framework of a research study is the framework that contains or supports the theory. The theoretical framework introduces and describes the theory that explains why the research problem occurs. Various theories and models are being used in the research to explain the awareness of phishing attacks among the students and what solutions can be made if they become phishing victims. This study also focused on the effect of three independent variables (social engineering influence, anti-phishing knowledge, and security concern) on the dependent variable (awareness of phishing among the people and the society).This will help the recognition of phishing attack activities in their development and provide a guide for the studies. The research method used for this research is the theoretical approach method. Applying a decision-making process enables specific phishing attack types and techniques. (B. Manya, 2019). The entire framework models are built to explain that individual behaviour is influenced by their beliefs and attitudes over particular things. The initial framework increased focus on the causes of phishing attacks among university students and organizations, such as the influence of social engineering, Anti-Phishing Knowledge, and security concerns.

The Technology Threat Avoidance Theory (TTAT) model further reveals that the combination of the perceived threat and protective efficacy also impacts I.T. users' avoidance motives. Numerous studies operating this model have proved that technology may significantly improve an individual's performance (MN Masrek, M., Jamaludin, A. and Awang Mukhtar, S. 2010). As a result, the framework represented in Figure 1 was employed to construct this investigation. Hence, this study investigates the knowledge and trust of I.T. users in their ability to resist phishing attempts and take protective actions. When I.T. users are well-versed in anti-phishing, security will be established. The researcher examined the relevance of ideas and their linkages in Phishing attacks knowledge by utilizing the input, process, and output model from The Technology Threat Avoidance Theory. The model further reveals that the perceived threat and protective efficacy combination will also impact the I.T. user's avoidance motive.

5 Conclusions

In conclusion, a theoretical framework limits the scope of relevant data by focusing on specific variables and defining the researcher's viewpoint in analysing and interpreting the data to be gathered, understanding concepts and variables. It demonstrates an understanding of theories and concepts relevant to the research topic and provides broader areas of knowledge under consideration. Also, the framework reflects a sense of theories and concepts pertinent to the research topic. The

framework's impact is based on the established theory behind improvement methods. Besides that, the framework can validate and challenge theoretical assumptions, facilitates understanding concepts and variables per the given definitions and builds new knowledge. In future, it would be interesting to see if the theoretical framework proposed in this study will be linked to other integrated frameworks to create a piece of new knowledge.

Acknowledgments

We thank the Faculty of Information Management, UiTM Puncak Perdana and Institute of Graduate Studies (IPSis) Universiti Teknologi MARA (UiTM) for supporting the publication of this paper.

References

Abed, T. M., & Abdul-Wahab, H. B. (2019). Anti-Phishing System Using Intelligent Techniques. *SCCS 2019 - 2019 2nd Scientific Conference of Computer Sciences*, 44–50. https://doi.org/10.1109/SCCS.2019.8852601

Anti-Phishing Working Group (APWG). (2018). Phishing activity trends report 2nd quarter 2018. Unifying the global response to cybercrime.

Baykara, M., & Gürel, Z. Z. (2018). Detection of phishing attacks. *6th International Symposium on Digital Forensic and Security, ISDFS 2018 - Proceeding*, *2018-January*, 1–5. https://doi.org/10.1109/ISDFS.2018.8355389

Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on Phishing Attacks. *International Journal of Computer Applications*, *182*(33), 27–29. https://doi.org/10.5120/ijca2018918286

Farhana, N., Zaharon, M., & Ali, M. M. (2021). *Factors affecting awareness of phishing among generation y*. *Asia-Pacific Management Accounting Journal, 16(2),* 410-444.

G. J. W. Kathrine, P. M. Praise, A. A. Rose and E. C. Kalaivani,(2019) "Variants of phishing attacks and their detection techniques," *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI*, pp. 255-259

Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. In *International Conference on Computing, Communication and Automation (ICCCA2016)* (pp. 537-540). IEEE.

Jain, A. K., & Gupta, B. B. (2016). A novel approach to protect against phishing attacks at client side using autoupdated white-list. EURASIP Journal on Information Security

K. D. Tandale and S. N. Pawar, "Different Types of Phishing Attacks and Detection Techniques: A Review," 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), 2020, pp. 295-299

Younis, Y. A., & Musbah, M. (2020). A framework to protect against phishing attacks. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3410352.3410825

Kamruzzaman , M., Islam, M. A., Islam, M. S., Hossain, M. S., & Hakim, M. A. (2016). Plight of youth perception on cybercrime in South Asia.*American Journal of Information Science and Computer Engineering*,

M. Khonji, Y. Iraqi and A. Jones, "Phishing Detection: A Literature Survey," in *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2091-2121, Fourth Quarter 2013, doi: 10.1109/SURV.2013.032213.00009.

Muniandy, L., Muniandy, B., & Samsudin, Z. (2016). Cyber security behaviour among higher education students in Malaysia. *Journal of Information Assurance & Cyber Security*. *2017*, 1-13.

Noorman Masrek, M., Jamaludin, A. and Awang Mukhtar, S. (2010), "Evaluating academic library portal effectiveness: A Malaysian case study", *Library Review*, Vol. 59 No. 3, pp. 198-212.

P. Liu and T. Moh, "Content Based Spam E-mail Filtering," *2016 International Conference on Collaboration Technologies and System (CTS)*, 2016, pp. 218-224

Patil, S., & Dhage, S. (2019). A Methodical Overview on Phishing Detection along with an Organized Way to Construct an Anti-Phishing Framework. *2019 5th International Conference on Advanced Computing and Communication Systems, ICACCS 2019*, 588–593. https://doi.org/10.1109/ICACCS.2019.8728356

Rao, S. R., & Pais, A. R. (2019). Jail-Phish: An improved search engine based phishing detection system. *Computers and Security*, *83*, 246-247.

Ripa, S. P., Islam, F., & Arifuzzaman, M. (2021). The emergence threat of phishing attack and the detection techniques using machine learning models. *2021 International Conference on Automation, Control and Mechatronics for Industry 4.0, ACMI 2021*, *0*(July), 8–9.

Sahoo, P. K. (2018). Data mining a way to solve Phishing Attacks. *Proceedings of the 2018 International Conference on Current Trends towards Converging Technologies, ICCTCT 2018*, 1–5. https://doi.org/10.1109/ICCTCT.2018.8550910

V.Bhavsar, A.Kadlak, & S.Sharma (2018). Study on Phishing Attacks. International Journal of Computer Applications. 182. 27-29.10.5120/ijca2018918286.