Borneo International Journal eISSN 2636-9826; Vol. 6 (1); 2023; 65-72
Published by *Majmuah Enterprise*
www.majmuah.com

A Study of Phishing Attack towards Online Banking

FATIN IZZATI FAMMY RIKZAN and MOHAMAD FADLI ZOLKIPLI
School of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah Darul Aman, MALAYSIA
Email: fatinizzatifammyrikzan@gmail.com | Tel: +60136068672 | Fax: +608123456 |

Received: February 23, 2023
Accepted: February 26, 2023
Online Published: March 01, 2023

Abstract

Online banking is a convenience system for people conducts their Internet-based financial activities. Online banking widely used by consumers as it can monitor their financial activities or accounts state easily through the website or mobile application. Unfortunately, this online banking has been targeted by the cyber-attacks with some security issues such as phishing attack. This phishing attack usually related with the social engineering skill to exploit the trust from consumers. Gaining crucial financial data and stealing confidential information of the consumers could be the reasons of the cyber-attacks being exploited towards online banking consumers. The Internet used during online banking transaction is one of the vulnerabilities that lead to the attacks. This phishing attack may cause consumers loss their trust towards bank companies as their confidential data being stole and modified by illegal resources. Because of this cyber-attack, several steps and security plans have been applied by the bank companies and consumers to prevent the phishing attack towards online banking. The social engineering related with phishing attack towards online banking and the countermeasure for phishing attacks will be discussed in this paper.

Keywords: Online banking; phishing attack; social engineering

1. Introduction

Online banking is a system where the consumers can do financial transactions directly from their bank account through digital platform such as computer or mobile phones as long as there is Internet connection. Based on the progressive evolution of information and communication technology in Malaysia, this online banking was introduced on 1st June 2000 to give the consumers effective ways to manage their banking account and financial transactions without going to counters physically (Ling, 2015). This system gives benefit to the consumers in saving time and energy as they are not required to go to the bank counter directly to do any transactions. Usually, the bank counters operations hours based on office hours, this will limit the consumers to do any transaction especially during urgent situation, but this is not an issue anymore with online banking system. The bank account can be access anytime and anywhere only with fingertips. In order to get access in using online banking service, the consumers need to register by creating user identification detail and password. The password and user identification detail is the key for the consumer access their online account bank. Because of that, the attacker attracted to steal these data from consumer by exploiting cyber-attack. According to (Haru, 2021), in Nigeria their online banking cyber-crimes that consists of hacking, spam mails, phishing attack, credit card deceit, phishing and fraudulent impersonator web. Phishing threats through social engineering also very common attack happen in Malaysia online banking (Gan, 2008).

Social engineering is defined as one of the easy methods in finding and gaining crucial information from targeted victim based on the skill or ability of the attackers, the attack basis is by exploiting weaknesses of the victim and the attacker collecting confidential and secrecy details either from individual or organization target (AL-Otaibi, 2020). This technique of social engineering is different compare to other cyber-attack as it does not involve any computer skills but only with techniques in manipulation other human in order get access into their sensitive information, stealing the crucial data, modifying the data and harming individual or organization. This social engineering can be done by attracting the victims to installing malicious files, downloading applications with injected malware which can expose their details unwillingly to the attacker that create those malicious sources. This type of attacks also refers to the phishing as the victims luring to click the link as it looks trustworthy even though it is harmful.

Phishing attack is a threats in the cyber security that created by the attackers to breach the confidential data of targeted victims. The phishing attack techniques is basically with creating the fraud websites by copying the interface of original page to confusing the user to unable detecting the difference of legitimate and counterfeit websites (Vanitha, 2022). By this fraud website, the attacker can collect the confidential data of the online banking if they click to the created malicious links. The links could be sending through emails, message or any social media platforms that serve links attachment.

In this paper, the study of the phishing attack towards online banking will be divided into 6 sections which are **Section 2** is literature review. **Section 3** is discussing on type of social engineering attack and related with phishing attack. **Section 4** is describing on type of phishing attack and techniques towards online banking. **Section 5** is about phishing attack countermeasure discussion and conclusion in **Section 6.**

2. Literature Review

Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case

According to **(Hasan, 2021)**, the study is about the readiness of Iraqi bank users towards the cyber-security that can exploit their database. There are several types of cyber-attacks towards the Iraqi private bank have been explained. Some of the cyber-attacks listed were hacking, distributed DoS attacks (DDoS) and phishing attack. This research conducted by questionnaires methodology to get the statistics of the results based on the cyber threats involved. The size of data sample is from Iraqi cities which are Baghdad, Karbala, Najaf and Babel. There were 51 respondents with 62.7% male and 37.3% female. These questionnaires were to study the readiness of the respondents towards cyber security. Table 1 shows the variance inflation factor (VIF) values of independent variables.

Table 1: VIF values of independent variables **(Hasan, 2021)**

Dependent Variable With:	Collinearity Statistics	
	Tolerance	VIF
Cyber stalking	.890	1.124
Hacking	.884	1.131
Phishing	.869	1.151
Cross site script	.927	1.079
Distributed DoS attacks	.816	1.226

In conclusion, based on the results from this paper, it shows that the customers of private bank in Iraqi are able to prevent the cyber-crime but still there are several of them worry about the cybercrime. Based on this paper, phishing attack is one of common threats to the online banking transaction. In future, the proper study of phishing attack countermeasure could be conduct to prevent the worries of consumers towards this phishing.

3. Social Engineering Attack

One of biggest threats in cyber security is social engineering. By social engineering, the confidentiality and sensitivity of important information can be exploiting by the attacker and use them for specific purposes such as blackmailing the victim or any bad intention in selling the data to the illegal market (AL-Otaibi, 2020). In social engineering attacks there are four types of stages which are the first is gathering data, second stage is relationship development, third is exploitation and fourth is execution without track by attacker (Koyun, 2017). Figure 1 shows the diagram of four stages of social engineering attack.

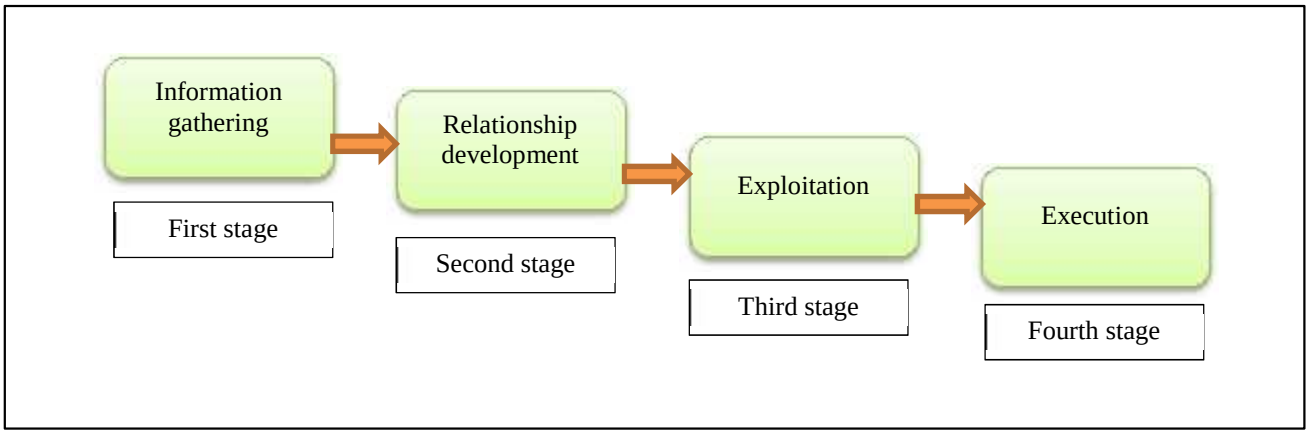


Figure 1: Four stages of social engineering

During information gathering stage, the attackers do a research towards the target victim to study their background by collecting information and detail from different resources. Some of the common resources are the website of the target, public documentation and direct interaction. This stage is important to obtain the information especially for individual target. In second stage, the attacker starting to make up conversation with the victim or any methods, to create relationship between them in order to analyse several ways to attract the excitement of the victim. Next, in exploitation stage, this purpose of stage is basically to establish stronger relationship with the target victim. The relationship between attacker and victim will be stronger with continuous interaction or dialogue to make sure the desired data success to be collect and complete the plan and built the software. Last but not least, the fourth stage which is execution. This stage is last step in social engineering attack that the attacker will execute the attack plan and directly cut the relationship with the target without their conscious of the data exploitation (Koyun, 2017).

Other than human based, in social engineering attacks there is computer based type. The human based is applied directly by an attacker towards the victim to gain the important data. This human based social engineering attack has limited amount of targets because of the less capacity can be create compared to the software-based type. In software-based social engineering, it is conducted by help from the system or devices such as computer, mobile phone and so on to get the information from the target. Social Engineering Toolkit (SET) is a part of software-based that usually applied to generate spear-phishing emails. Based on this type of social engineering, the phishing attack obviously has relationship with the social engineering.

Phishing attacks tricks that commonly used through social engineering are spear phishing, vishing phishing, whaling phishing, voice response phishing and last but not least business email phishing. These phishing attacks go through the social engineering because of the after process of the attackers gain the important information and authorization from the victims. The social engineer will use the data stole from the targets and manipulate them. For example, the social engineers can use the data to changes emails, forward emails, modify the meeting schedule without the owner concerns for bad purposes. The attacker can play game with all the data they have with sending fake email that look like a real email from a legit account to the other ordinary employee and send them malicious links. As the victims download the link files, the attacker directly can access the company devices and steal the information or modify them.

4. Phishing Attack

Phishing attack is one of security issues that used by the hackers to gain information from the other people. This phishing attack is worked with the act like the trustworthy sources or entity in online platform to manipulate the victims to obtain sensitive data, including credit card information, password and a username. The attackers will claim their selves as the person or company from the famous social websites, online payment process or else that usually used to attract the public without any suspicious. Phishing attacks commonly target the emails, telephone, banking details, credit card information and account passwords. Social Engineering is being used by the attacker or phisher in stealing personal data and account information of the targeted victim. Phishing attack can divided into two parts which are deceptive attack and technical subterfuge. In this study will be focus on the deceptive attack which is related more to the social engineering in manipulating human psychology compare to the technical method (Alkhalil, 2021). There are several types of attack from deceptive phishing which are phishing email, spoofed website, phone phishing and social media phishing as shown in Figure 2.

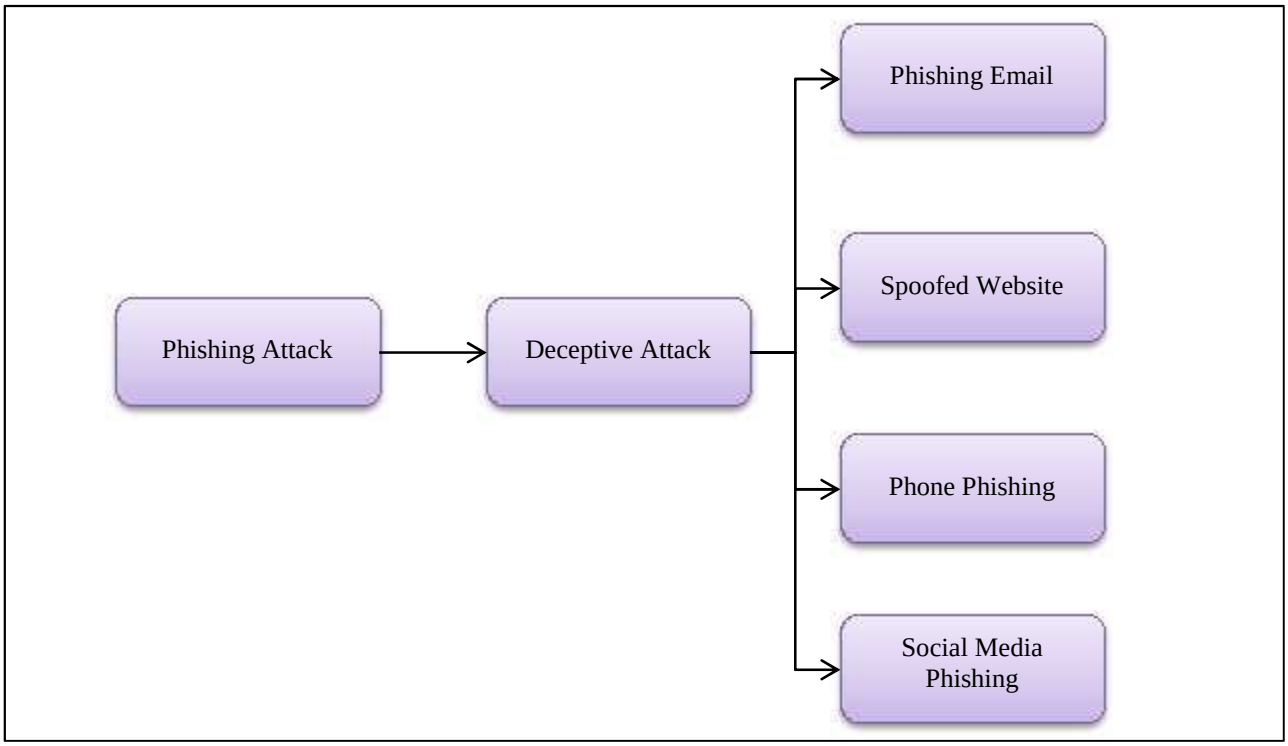


Figure 2: Deceptive Phishing Attack

Phishing Email: Phishing is always being used by attacker to hack an email. Email phishing is when the phisher send malicious link to the victim via email that look alike their important document such as bank account statement, if the victim click the link provided and fills the detail, automatically their information filled received by the phisher. The phishing general methodologies in email phishing are explained in Figure 3 (Bhavsar, 2018).

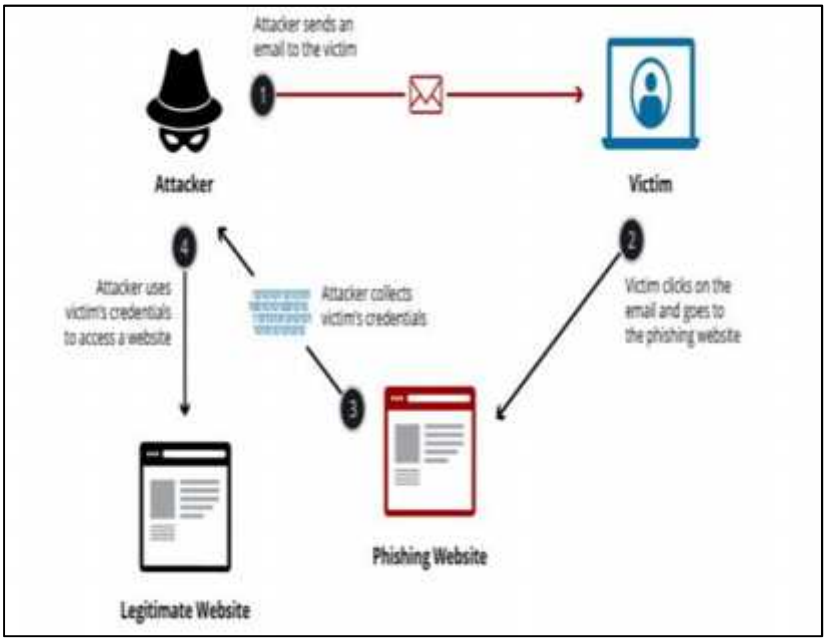


Figure 3: Phishing attack methodologies (Sources: (Bhavsar, 2018))

Based on the diagram in Figure 3, the first step shows that the attacker sending an email with malicious link to the target victim. Next, as the victim clicks the link he or she will directly bring to the fraud websites created by the attacker. If the victim fill up the details require in the website, the attacker directly get all their details. Lastly the fourth

step, as the details get by the attacker they will use it to access any victim's credentials to access the website. This phishing attacks will make the victims loss integrity and confidentiality towards their privacy data.

Spoofed Website: In spoofed website, the webpage the phisher makes will looks genuine and similar with the legit website. The link of this fraud website is being shared through the email or any media sources to the users, when they click the website link and continue interacting with the spoofed websites, there is huge possibilities for their sensitive detail being disclosed and steal by the phisher.

Phone Phishing: Phone phishing generally called as *Vishing* or *SMishing* as it use phone call or text messages as medium. The attacker will pretend as someone trusted or that the victims know to deal with them. For example, any transaction from online banking will generate PIN numbers for the users. They may get a persuasive security alert notice that asking the target to contact a specific phone number from bank to retrieve sensitive information. The victim may be led astray by an actual source in the email or text. The attacker might access the victim's messaging account using their personal data information and do phishing to other users in their contact list.

Social Media Phishing: This is one of the latest methods of cyber-attack to generate phishing attack as nowadays most people active on social media platforms. Hijacking social media account, scams, malware distribution and impersonation attacks towards victims are several ways in social media phishing. Even this attack popular among phishers, as social media remains beyond the network boundary, it requires longer time compared to traditional methods for detecting and mitigate these threats (Alkhalil, 2021).

Phisher conducted various techniques of phishing attacks towards the online banking users to exploit their confidential data. But, based on the recent statistic from (Verizon2021, 2021), 96% of the phishing attacks were conducted by sending emails with malicious links created that bring to malicious webpage or a file attachment. By clicking the malicious link in the phishing email will result in client financial damage and adversely harm good name and reputation of the bank. The technique of phishing email created by the hacker is sending fraudulent emails to internet banking users. The attacker targets the users' privacy detail such as password, login username, security code and financial details. Figure 4 shows phishing email example that consist legitimate bank logo on page to make it more genuine. The email state a warning to the customers that their account have been suspended and need to payment by clicking provided link.



Figure 4: Phishing email towards online banking (Source: https://www.pbebank.com/Personal-Banking/Banking/E-Channel/PBe-Online-Banking/scams2_2.aspx)

The phishing email could contains with link or file attachments that direct the users to the malicious external website that already being programmed by the phisher to steal the customers' sensitive information and banking details (Manoharan, 2022). If people are more aware of the kind of phishing attacks being sent to them, they can avoid falling victim to attackers. Then, as the customers or users identify the phishing emails; they can mark the phishing email, directly delete them or block the sender to prevent receiving same phishing email in future.

5. Phishing Attack Countermeasures

All kind of cyber-attacks have their countermeasures or preventing methods can be applied to avoid being attack. This phishing attack towards online banking also can be preventing with several steps either from the bank or individual. Based on **(Alsayed, 2017)**, there are several phishing attack countermeasures can be used to prevent the attacks. There are email and web page personalization, protection software, two-factor authentication and increasing customer awareness.

5.1 Email Personalization

The bank companies need to include the personalized information of email with all the legitimate list of communication for their customers. Personal identifiable information need to be implementing to help customers easily identify the message is from phishing attacks or legitimate message. The personal identifiable details may involve the customers' name or any unique details shared between bank and the users. Every email or message should be identify and personalize with legit note or recipient before being send to the customers. Bank users can ensure that the email is legit from the bank with the implementation of the personal identifiable information this will reduces the rate of phishing email threats towards online banking. As the detail of the customers or users does not being included and use the personalization method, it can reduce the phishing deceptiveness. Even this technique may be difficult to apply, but it is effective to safeguard the customers' credential data.

5.2 Web Page Personalization

Web page personalization also one of the personal identifiable information that can be implement by the bank. For this kind of personalization, the image or text will be request by online banking users along with their usernames and passwords. It means that in order to access the bank web page, customers must first navigate through two pages for personalization. Usually, the first page consists of the users' username validation and the personalized page for entering password after the name is valid. The second page, the users will be asked to confirm the image or phrases they chose during the first time they created the bank account. The bank users must be reminded by the bank to not type in their password if the image shows on the second page is different with the chosen one. The phisher will not success to do phishing attacks as they do not know about the personalized data and unable to replicate it when generating to connect the deceptive websites.

5.3 Two-factor Authentication

Two-factor authentication is an effective way to authenticate customer identity compared to the previous method which is single-factor authentication. The single-authentication safeguard is weak because it is vulnerable to phishing attacks, which enable hackers to simply circumvent the authentication. Because of that, bank comes out with the two-factor authentication especially related with high risk transactions. In two-factor authentication, the users must confirm their identities with two separate pieces of proof. The first factor basically involves hardware or software that automatically provides electronically generated passcode. The second factor is a private password that only knows by the users. The two-factor authentications give the bank users stronger authentication system when they accessing the online banking. This countermeasure can reduces the chance of phishing attacks because it is difficult for the attackers to capture the second factor even they already get the first factor detail.

5.4 Customer Awareness

Bank companies should provide awareness campaign towards the bank users. This preventing step is very important and reasonable to be implementing because the most phishing attack started with fake email. The education about the danger of phishing email can reduce the number of customers from clicking any malicious links frim the phishing email as they already know how to identify and aware the fraudulent emails. This awareness can be conduct by updating the customers frequently through the website or bank mobile application. The bank users can identify legitimate emails and web sites if the banks regularly updates about the phishing attacks awareness. Then guidelines also can be provide to the customers to make sure the customers have being informed about in which ways bank will use to communicate with them. Basically, the guidelines divided into two parts which are during the first registration in document form and the second guideline usually provide as "security instruction" on the websites of the bank. If the awareness of phishing attack among the bank users increase, the number of the phishing attack will be reduce. This prevention step is very effective depends on how the customers level of awareness.

6. Conclusion

Phishing attacks are a social engineering that nowadays actively used by the attackers to attack the individual or organization. Deceptive phishing attacks are the most related to the social engineering which some of them being used by attacker to attack the online banking users. Online banking involves many kind of risk as it open to Internet connection that can lead to the financial loss and data being stolen by the attackers. Some countermeasures have being explained to prevent and reduce the phishing attack to happen towards the online banking users. The phishing attack is impossible to be fully prevent but it can be reduces with the presence of awareness among the bank users and precautions steps taking by the bank companies.

Acknowledgments

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of Ethical Hacking & Penetration Testing Research Project. This work was supported by Universiti Utara Malaysia.

References

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future internet*, *12*(10), 168.

Aldawood, H. S. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, *11*(3), 73.

Aldawood, H. S. (2020). An advanced taxonomy for social engineering attacks. *International Journal of Computer Applications*, *177*(30), 1-11.

Ali, G. A. (2020). Two-factor authentication scheme for mobile money: A review of threat models and countermeasures. *Future Internet*, *12*(10), 160.

Alkhalil, Z. H. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*.

AL-Otaibi, A. F. (2020). A study on social engineering attacks: Phishing attack. *Int. J. Recent Adv. Multidiscip. Res*, *7*(11), 6374-6380.

Alsayed, A. B. (2017). E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. *International Journal of Emerging Technology and advanced engineering*, *7*(1), 109-115.

Alzahrani, A. (2020). Coronavirus social engineering attacks: Issues and recommendations. *International Journal of Advanced Computer Science and Applications*, *11*(5).

Bansla, N. K. (2019). Social engineering: A technique for managing human behavior. *Journal of Information Technology and Sciences*, *5*(1), 18-22.

Bhavsar, V. K. (2018). Study on phishing attacks. *Int. J. Comput. Appl*, 27-29.

Bhusal, C. S. (2021). Systematic Review on Social Engineering: Hacking by Manipulating Humans. *Journal of Information Security*, *12*, 104-114.

Deshpande, A. P. (2021). Detection of phishing websites using Machine Learning. *International Journal of Engineering Research & Technology (IJERT)*, *10*(05).

Gan, G. G. (2008). Phishing: a growing challenge for Internet banking providers in Malaysia. *Communications of the IBIMA*, *5*, 133-142.

Haru, A. H. (2021). Challenges of Cybercrime on Online Banking in Nigeria a Review. *IDOSR JOURNAL OF BANKING, ECONOMICS AND SOCIAL SCIENCES*, 17-23.

Hasan, M. F.-R. (2021). Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case. *Social Science and Humanities Journal*, *5*(8).

Jansen, J. L. (2016). hishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), 79.

Koyun, A. A. (2017). Social engineering attacks. *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*, *4*(6), 7533-7538.

Lim, W. H. (2020). Phishing security: Attack, detection, and prevention mechanisms. *In Proceedings of the International Conference on Digital Transformation and Applications*, 8.

Ling, C. I. (2015). Users satisfaction towards online banking in Malaysia. *International Business Management*, *9*(1), 15-27.

Manoharan, S. K. (2022). o click or not to click the link: the factors influencing internet banking users' intention in responding to phishing emails. *Information & Computer Security*, *30*(1), 37-62.

Ramli, F. A. (2021). Mobile payment and e-wallet adoption in emerging economies: A systematic literature review. *Journal of Emerging Economies and Islamic Research*, *9*(2), 1-39.

Sumner, A. ,. (2019). Mitigating phishing attacks: an overview. *In Proceedings of the 2019 ACM Southeast Conference*, 72-77.

Sumner, A. Y. (2019). Mitigating phishing attacks: an overview. *In Proceedings of the 2019 ACM Southeast Conference*, 72-77.

Vanitha, G. (2022). Detection of Phishing Attack. *International Journal of Research Publication and Reviews*, 569-573.

Verizon2021. (2021). *2021 DBIR master's guide*. Retrieved February 7, 2023, from https://www.verizon.com/business/en-gb/resources/reports/dbir/2021/masters-guide/