2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC) | 979-8-3503-7304-2/24/$31.00 ©2024 IEEE | DOI: 10.1109/KHI-HTC60760.2024.10482040

Understanding Human Behavior in Phishing Attacks Across Diverse User Groups: An Ethical Hacking Analysis

Fahad Hussain
Department of computer science
International Islamic University Malaysia
Gombak, Malaysia
Kingfahad414@gmail.com

Rayyanur Rahman
Department of computer science
International Islamic University Malaysia
Gombak, Malaysia
rayan4rahman@gmail.com

Zainab S. Attarbashi
Department of computer science
International Islamic University Malaysia
Gombak, Malaysia
Zainab_senan@iium.edu.my

Wafa Hussein Naser Fadaq
Department of computer science,
Management & Science University,
Saudi Arabia
wf.fadak@gmail.com

Manar Mustafa
Department of computer science
International Islamic University Malaysia
Gombak, Malaysia
manar.m2015@gmail.com

***Abstract*— In the face of increasingly advanced cyber threats employing different social engineering methods, there is a crucial need to comprehend how individuals respond to deceptive emails and messages. This research investigates the analysis of human behavior across various user groups by utilizing phishing emails and messages as testing tools. By employing ethical hacking methodologies, the study studies and executes realistic phishing attacks, aiming to observe and comprehend how individuals fall victim to social engineering tactics, resulting in financial losses and compromised passwords. In order to collect data, a survey was prepared together with a fake website (IIUM Wi-Fi login page) to provide insights into the vulnerabilities inherent in user interactions with phishing attempts. The findings highlight that a lot of people tend to click on unknown links out of curiosity, which can easily make them a victim of social engineering attack. The results suggest that around 84% of the targeted respondents consider whatsapp /messages to be very important in daily communication. However, 25.5% of them have clicked on the phisihing link via whatsapp message and inserted their login details. Findings uncovered potential vulnerabilities and a 28.6% impulsivity rate. A phishing experiment illustrated cybersecurity risks, underscoring the need for awareness and education.**

***Keywords*— Social Engineering, Human Behavior, Phishing Attack, Ethical Hacking.**

I. Introduction

In this era of rapid technological progress and pervasive internet usage, individuals must be aware of their privacy, particularly while navigating online spaces. The increase in social engineering scams is a concerning matter, reflecting an alarming increase in individuals falling victim to deceptive tactics. According to AAG Report [1], an estimated $2.7 billion was stolen via phishing attack in US alone in year 2022. Furthermore, a significant portion of emails, constituting 55%, is identified as spam, often lead to various malicious activities. Social engineering encompasses a spectrum of techniques employed by cyber attackers, involving emails, websites, messages, and malware, with the primary objective of manipulating unsuspecting victims, typically ordinary citizens. This manipulation aims to extract sensitive personal information, establish trust, and analyze behavioral patterns for malicious ends.

Individuals with limited knowledge about networks and security often become susceptible to scammers who exploit their lack of awareness, resulting in the unintentional disclosure of personal data. These attackers try to sabotage the use of attractive emails with catchy titles to manipulate users. Once users obliges to these tactics, attackers gain access to sensitive details such as passwords and bank information. In more severe cases, attackers may install malware on the user's computer or phone. Notably, vulnerability to social engineering is not confined to regular users; even cyber experts and major companies have fallen prey to such attacks. One of the famous incidents is the phishing email attack on Google and Facebook, leading to the theft of approximately $100 million. The perpetrator, Evaldas Rimasauskas and his team set up a fake company and started sending phishing emails to the employees at Facebook and google, ultimately luring them to pay to his company, but he set up his own different bank accounts under his business [2].

According to [3], social engineering is a manipulation technique exploiting human error to illegally obtain private information, access, or valuables. It has emerged as a highly effective method for scammers to achieve their objectives with relative ease. Often, scammers deploy simple tactics, such as sending phishing emails or SMS, wherein they impersonate important figures or reputable organizations, urging users to click on specific links. Alarmingly, 91% of attacks by sophisticated cyber criminals initiate through email, highlighting the concerning reality that attackers manage to succeed despite the presence of multiple spam filters and protective measures on computers [4].

Unlike any other tools, social engineering is more powerful because it involves human interaction where the user is psychologically tricked into giving sensitive information to the attacker without realizing. The inherent danger of social engineering lies in its ability to penetrate security measures

979-8-3503-7304-2/24/$31.00 ©2024 IEEE

that are typically robust and up-to-date. Even if a company diligently maintains cutting-edge hardware, keeps software security consistently updated, and operates the most secure network server, it remains susceptible to social engineering. This vulnerability arises from the fact that social engineering sidesteps traditional security infrastructures, directly targeting and extracting information from users.

The examination of human behavior plays an important role in safeguarding against social engineering attacks as these exploits heavily use human nature and feelings. A successful social engineering attack often manipulates users by instilling a false sense of security, capitalizing on the inherent human tendency to trust information at face value without skepticism. For example, in scenarios where customer assistance is needed, employees commonly accept the first identity presented by the customer without cross-referencing, showcasing the inherent human leaning to trust and provide information readily. Understanding and studying these human behaviors are instrumental in fortifying defenses against social engineering, allowing for the development of targeted awareness programs and security protocols that address the specific vulnerabilities inherent in human interactions.

There can be many different forms of attacks using social engineering, the main form of attack involves phishing where the attacker will pretend to be a trustworthy individual to make the victim reveal sensitive information. There are many different types of phishing attacks which are detailed in Table 1.

TABLE I. DIFFERENT TYPES OF PHISHING ATTACKS

Attack Name	Description
Email Phishing	Attackers send deceptive emails appearing to be from a reputable source, tricking recipients into revealing sensitive information.
Spear Phishing	A targeted form of phishing where attackers tailor messages for specific individuals or organizations, often using personalized information.
Vishing (Voice Phishing)	Attackers use phone calls to impersonate trusted entities, convincing individuals to disclose sensitive information over the phone.
Smishing (SMS Phishing)	Phishing attacks conducted via text messages, where users are lured into clicking on malicious links or providing sensitive information.
Whaling	Similar to spear phishing, but specifically targeting high-profile individuals such as executives or key decision-makers within organizations.
Clone Phishing	Attackers create a replica of a legitimate email, modifying it to include malicious content or links, and then send it from a seemingly trusted source.
Link Manipulation	Malicious links are disguised to appear legitimate, leading users to fraudulent websites where sensitive information is collected.
Search Engine Phishing	Cybercriminals manipulate search engine results to lead users to malicious websites designed to collect personal information
Ransomware Attacks	Phishing emails may contain malicious attachments that, when opened, deploy ransomware, encrypting the victim's files until a ransom is paid.

Malaysia is among the top countries affected by phishing attacks. According to Cynthia [5], In the first two quarters of 2022, Kaspersky found a total of 195,032 payment system-related phishing operations in Malaysia, including 108,755 in the first quarter and 86,277 in the second. A total of 48,850 internet scams, or 68% of the 71,833 commercial crime cases registered from 2020 till May of this year, were reported as revealed by the inspector-general of police. Additionally, Kaspersky products also found and stopped 91,895 phishing attempts targeting Malaysian e-commerce stores, as well as 27,458 attempts related to banks [5]. It can be clearly seen how the scammers are nonchalant in trying to unleash their phishing attacks to different groups of people in many different ways and if people are not made aware of these attempts, loss of credentials and money will become a common issue.

The aim of this research is to study human behaviours using a real phishing attack. This was done by the following:

- analyze human behaviour regarding social engineering.
- design a system/app to keep track of users that are clicking on a phishing link.
- To use the built system to analyze the results in order to find what type of messages attract different groups and who needs to get cyber awareness training in the future.

II. Related Works

There are many researches studied the human reactions to phishing attacks. Reddy and Venkata [6] used data mining technique and created a browser extension called gemini. The main purpose of it is to protect the users from phishing attacks. They deployed multiple Gemini prototypes as browser extensions for Internet Explorer, Firefox, and Chrome, and did rigorous tests on numerous genuine and fraudulent websites. Their test findings demonstrate that Gemini can achieve 0% false negative rate, 1% false positive rate, and successfully prevent access to a phishing site before a vulnerable user starts to submit personal credentials.

Tripti et al. [7] attacked ethical hackers who use the system to steal private information from any firm by creating a fake environment which they created using Kali and metasploit framework. They employed the Kali Linux Operating System (OS) tool to accomplish these ethical hacking and penetration testing, doing both server-side and client-side exploitations to better understand the process. Finally, they have suggested security upgrades and mitigating actions to counter hacking attacks.

Devi and Kumar [8] with their experiment on testing weakness of web applications using ethical hacking with tools like OWASP and ZAP found weaknesses on most of the areas of the domain.They collected their data from many places such as hospitals, government organizations, schools. They then performed vulnerability testing on 100 websites using host id/hostname. However, they only found medium and low level risk on these websites with no high level risk.

Larfield and Guest [9] built an ethical hacking site for learning and student engagement where students were asked to build a capture the flag using LAMP (Linux, Apache, PHP, and MySQL) stack. They managed to get 3 outcomes from the experiment, identifying common attack vectors, creating platforms for exploiting web-based technology and evaluating

979-8-3503-7303-5/24/$31.00 ©2024 IEEE

how a given attack can be mitigated to prevent future exploitation.

Butavičius et al., [11] used a mixed-methods approach, combining a survey and a laboratory experiment, to study the effectiveness of social engineering tactics in phishing and spear-phishing emails. The results indicated that social engineering tactics, such as creating a sense of urgency or using a trusted sender, were effective in increasing the likelihood of individuals clicking on phishing links. The limitations of this study include the use of a simulated phishing scenario, which may not fully capture the complexity of real-world phishing attacks, and the use of a small sample size of participants.

Musuva et al,. [12] used a naturalistic methodology, in which participants were exposed to real-world phishing emails, to study susceptibility to social engineering attacks. The results indicated that individuals with lower levels of phishing self-efficacy were more likely to fall victim to phishing attacks. The limitations of this study include the use of a small sample size of participants, and the focus on a single aspect of susceptibility to social engineering attacks.

Albladi & Weir [13] used a survey to study the relationship between user characteristics and judgment of social engineering attacks in social networks. The results indicated that individuals with higher levels of education and experience with technology were less likely to fall victim to social engineering attacks in social networks. The limitations of this study include the use of a self-reported measure of susceptibility to social engineering attacks, which may not accurately capture actual behavior.

James Nicholson et al., [14] used a laboratory experiment to study the effectiveness of using social salience, or the degree to which a message is relevant to an individual's social network, as a means of improving phish detection. The results indicated that individuals were more likely to detect phishing emails when they were more socially salient. The limitations of this study include the use of a simulated phishing scenario, which may not fully capture the complexity of real-world phishing attacks, and the use of a small sample size of participants.

Halevi et al., [15] used a real-world study of spear-phishing attacks to investigate the relationship between personality, phishing self-efficacy, and vulnerability to spear-phishing attacks. The results indicated that individuals with higher levels of phishing self-efficacy were less likely to fall victim to spear-phishing attacks, but that personality factors did not play a significant role in vulnerability to these attacks. The limitations of this study include the use of a small sample size of participants and the focus on a single aspect of susceptibility to spear-phishing attacks.

Gupta et al. [16] applied multiple penetration testing on their own organization in an attempt to perform ethical hacking. They applied techniques like sniffing, phishing, malwares, windows exploiting and many other techniques to find the vulnerabilities within their organization. They managed to find loopholes in their websites and other parts of their organization however, they did not provide many diagrams of their results confirming the successful penetration testing using ethical hacking. Table 2 summarize the related works

TABLE II. SUMMARY OF RELATED WORKS

Ref.	Methodology used	Results	Limitation
[6]	Developed a browser extension called Gemini to protect users from phishing attacks	Research work aimed to present data mining methods to construct a model in order to protect against phishing attacks.	Focused on the technical aspects to prevent the phishing emails
[7]	Created a dummy environment to attack ethical hackers who exploit the system to get confidential information from any company. Used metasploit to create a payload to access the company laptops and mobile phones	Successfully used the 2 types of exploit, client-side and server-side exploit Successfully gained access to the victim's computer.	The tests are done in a dummy environment assuming the users have windows 7 and use android. A test on other operating systems would've been better as well with phones other than android as well.
[8]	Data was collected from Hospitals, Engineering colleges, Government organizations, Schools, Healthcare Companies, Business Organization, Sports, Banks, Financial Organization, IT Industries, and then vulnerability analysis and assessment were executed for 100 websites using hostname/ host ID. The scanning process was performed on the kali Linux platform using penetration testing on the top ten websites of each domain.	Using penetration testing, security weakness has been detected in all areas of domains finding medium and low-level alerts with the OWASP ZAP tool The experiment detected vulnerabilities like X-XSS-Protection header is not defined, Uncommon header found, SSL and the strict transport-security HTTP header is not defined, Server leaks inodes via ETag, Retrieved x-powered by a header from the Nikto tool than from OWASP ZAP	Detailed results and analysis without much limitations. Should've used more websites, preferably vulnerable websites to obtain a high-level risk as the OWASP tool only obtained low and medium-level risk
[9]	Students in a senior level undergraduate ethical hacking class were tasked with the development of a capture the flag platform built using the LAMP (Linux, Apache, PHP, and MySQL) stack that scored participants' progress while exploiting a vulnerable website.	Identify common attack vectors on web sites and methods to rectify the discovered vulnerabilities. Create attack platforms for exploiting web-based technologies. Evaluate how a given attack can be mitigated to prevent future exploitation.	The authors focused on the CTF platform and uses techniques like password cracking, SQL injections etc, however, the authors mentions that more CTF flags like steganography, encryption etc, should've been created as well to broaden the experience of the students
[10]	Wifi password cracking, windows exploiting, remote access tool, sniffing, spoofing, phishing,	Successfully implemented all the mentioned techniques onto their organizations network to find out the loopholes in their network	Explains more about the definitions rather than results of the experiments.

979-8-3503-7303-5/24/$31.00 ©2024 IEEE

	system hacking and security, cryptography and steganography.		Mentions that all techniques were implemented successfully, without details.
[11]	A sample of 121 students from different fields of study were experimented using 12 emails, which were either genuine, phishing or spear-phishing emails. Participants were shown each email separately and were asked to provide a 'Link Safety' judgment	The participants were unable to reliably distinguish between spear-phishing and genuine emails when the email contained reference to an authority figure.	This study was conducted on a very limited size of sample who are limited to students only.
[12]	The research used a field study experiment to stage a phishing attack targeting a university population of 4483 of which 241 participated.	Data collected on the backend database indicated a total of 98 clicks on the phishing hyperlink.	Some of the limitations of this study was, not enough of the targeted users received the email, some of the sample used the university email only for official work related to the university and had alternate email address for personal use.
[13]	An invitation email was sent to the selected experts asking them to participate in the study. The second phase was conducted 1 month later. An email was sent to 20 information security experts, all of whom were academic lecturers in Saudi Universities	The survey results revealed that the perceptual factors are generally very important factors to consider in relation to user susceptibility to social engineering.	All the participants of this study had a general background of information security.
[14]	In this research an online experiment via Amazon's Mechanical Turk was set up where participants were asked to view 18 emails (6 phishing, 12 real) and decide whether each email represented a genuine message or a phishing message.	It was found that participants were under-confident in their decisions when presented with genuine emails, but were overconfident when presented with phishing emails. It was also found that participants who scored high on the trait of dysfunctional Impulsivity were less accurate in identifying phishing emails and made faster decisions than those scoring low for the trait.	All of the participants in this study were already informed prior about the phishing experiment, participants were unable to directly interact with the system, some of the participants did not receive both the email, so there was a disadvantage for some of the participants.
[15]	The participants filled out a survey. In the second part, a phishing email was sent to them.	Out of the 40 participants who filled the questionnaire, 25 clicked on the link and 12 clicked on the 'download plug-in' button. Overall, 30% of the participants were phished	In this study, a specific type of message was used in the process of phishing, different types of message may have different emotional responses from different types of people.

III. Methodology

In order to understand and study the human behaviour of the target users, a self-structured questionnaire was prepared in the form of an online survey. A stratified sampling method for the survey was used because the aim is to collect information from different faculties at International Islamic University Malaysia (IIUM) from different fields of study, and also interview different users from different Faculties. Figure 1 shows the methodology of this research.

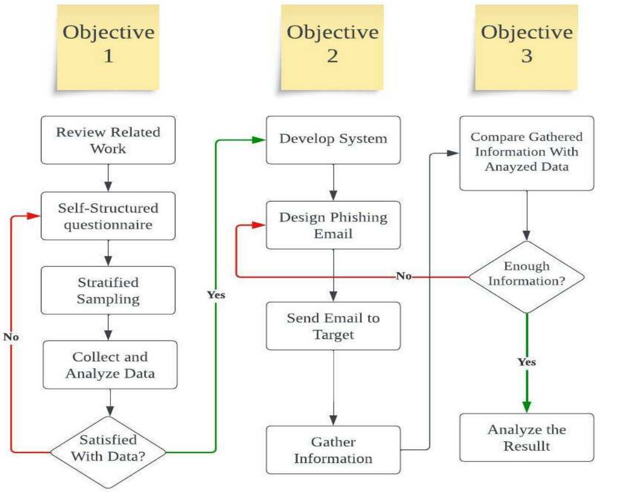


Fig. 1. Methodology flowchart

Based on the responses from the survey, the data was analysed to find out the possible weaknesses and the level of awareness of the different groups of participants. Many questions focused on the personality of the participants, the preferred communication methods, type of emails/messages they often receive, and their level of awareness about cyber-attacks. As shown in figure 2, 28.6% of the respondents are impulsive people. This information is important to know the targeted group better, as impulsive people tend to act without thinking about the outcome. Figure 3 shows that most of the participants receive email from shopping sites but also a large number of students receive email from lecturers and IIUM. And around 22% of the respondents are maybe or not aware of phishing attacks as shown in figure 4.

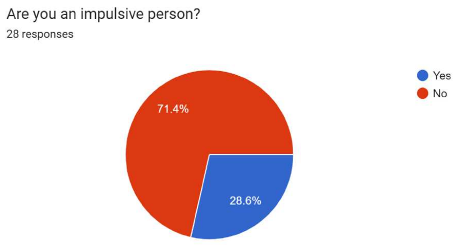


Fig. 2. Example of survey's answers to know the participants personalities

979-8-3503-7303-5/24/$31.00 ©2024 IEEE

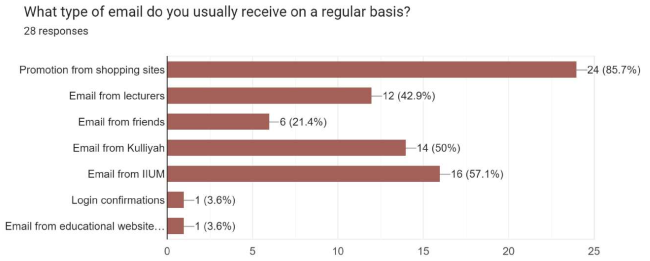


Fig. 3. Example of survey's answers about the type of emails received by users

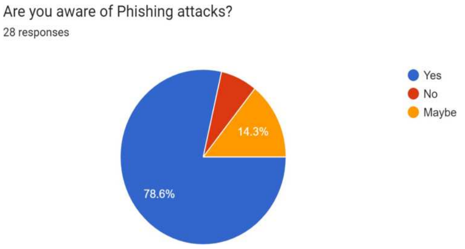


Fig. 4. Example of survey's answers about the level of awareness

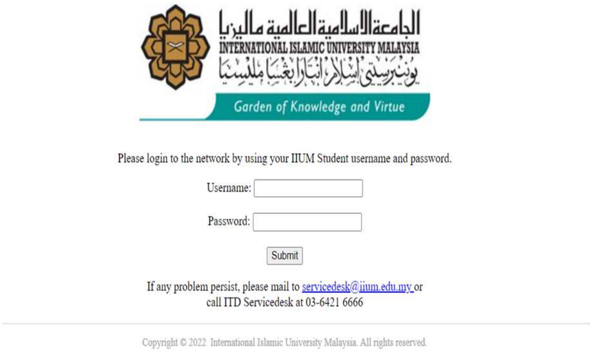
Based on the results, the phishing webpage that resembles the IIUM Wi-Fi login page was developed using html, JavaScript, and with the help of other tools such as API and chatbots. The purpose of this fake webpage is to capture information from the victim after they click on the link from the phishing email and type in their information. To store collected data, Telegram chatbot was used to send automated messages to any phone as soon as anyone inputs any information on the phishing page.

Later, the phishing page was published at Netify web hosting service. This host enables HTTPS encryption for any sites which will not raise any suspicions when anyone clicks on the link.

The link to the phishing page was attached at the end of the survey where the participants who completed the survey will be tricked to click on the link. As soon as they click the link they will be redirected to the phishing page where they will be asked to input their Wi-Fi login. For this study purpose, the SHA-256 encryption was implemented on the password field in the phishing page to protect their passwords. Only the user number was collected from the phishing page. The goal is to just identify the participant and relate them to the survey and compare their inputs from the survey to analyse and compare their answers to their action.

A spoofed webpage shown in figure 5 was built resembles the official IIUM wifi login page. After the user clicks on the link from their emails/message, they will be redirected to this webpage that looks like a genuine webpage and asks for information from the user. After the user inputs their information, in the backend of this page, a keylogger has been setup which captures each individual key presses and sends them to a webhook site.

As shown in figure 6, the users information have been collected once they input their details in the login page. The password could ne collected as well to show what will the real attacker get, however it was encrypted to follow the ethical codes.


INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA
Garden of Knowledge and Virtue
Submit

Please login to the network by using your IIUM Student username and password.

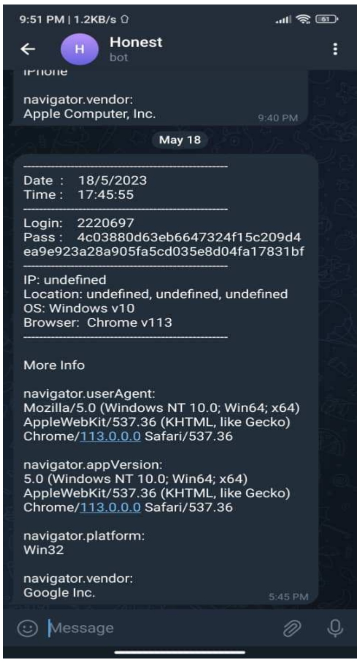
Username:

Password:

If any problem persist, please mail to servicedesk@iium.edu.my or
call ITD Servicedesk at 03-6421 6666

Copyright © 2022 International Islamic University Malaysia. All rights reserved.

Fig. 5. Spoofed IIUM wifi login page



```
iPhone

navigator.vendor:
Apple Computer, Inc.                       9:40 PM
```

```
----------------------------------------
Date :   18/5/2023
Time :   17:45:55
----------------------------------------
Login:   2220697
Pass :   4c03880d63eb6647324f15c209d4
ea9e923a28a905fa5cd035e8d04fa17831bf
----------------------------------------
IP: undefined
Location: undefined, undefined, undefined
OS: Windows v10
Browser:  Chrome v113
----------------------------------------

More Info

navigator.userAgent:
Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/113.0.0.0 Safari/537.36

navigator.appVersion:
5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/113.0.0.0 Safari/537.36

navigator.platform:
Win32

navigator.vendor:
Google Inc.                                5:45 PM
```

Fig. 6. Chatbot where login information is sent

IV. Results and Discussion

This research targeted 56 users with a phishing link that was embedded in a dummy IIUM Wi-Fi login page. Following are the key points analysed from their responses:

A. Do you trust IIUM websites?

Figure 7 shows the percentage of users who consider IIUM websites to be trustable at a certain point where 67.3% said they don't check the URL before using the websites. Whereas 32.7% says that they check the URL while using these websites.

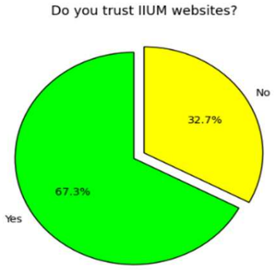


Fig. 7. Participants answers to question A

979-8-3503-7303-5/24/$31.00 ©2024 IEEE

B. *Are you aware of phishing attacks?*

Figure 8 shows that at least 21.8% users are not aware or maybe aware of phishing attacks. 78% users are aware of phishing attacks which helps them prevent from being a victim of scam.

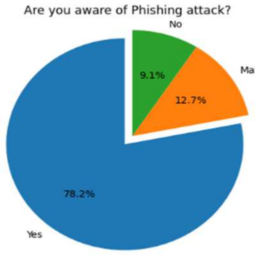


Fig. 8. Participants answers to question B

C. *Do you think you need to be more aware of internet scams?*

Figure 9 shows that 89.1% users wished to be made more aware of phishing attacks whereas 10.9% users suggest that they are already aware of these attacks and do not need further awareness.

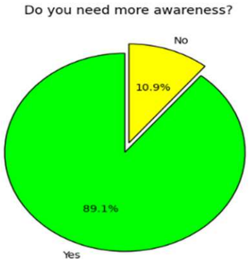


Fig. 9. Participants answers to question C

D. *Did you ever receive any type of phishing Email/Message?*

Figure 10 suggests that 45.5% users have not come across any type of phishing email/messages. 54.5% users have come across phishing email/messages.

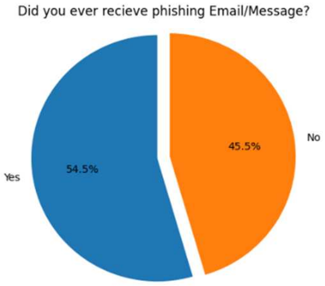


Fig. 10. Participants answers to question D

Out of 55 users, 14 users have clicked the embedded link in the phishing email and input their details. From figure 11, it can be observed that 25.5% of the users have input their details in the fake login page.

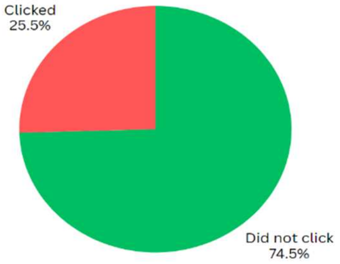


Fig. 11. % of user who input their details in the login page

V. Conclusion

In the face of escalating cyber threats and advanced social engineering techniques, this research trys to understand how individuals respond to deceptive emails and messages. Employing ethical hacking, the study executed realistic phishing attacks to observe and comprehend susceptibility to social engineering. The survey and simulated phishing attempts revealed that a significant number of individuals, driven by curiosity, clicked on unknown links, making them susceptible to attacks. Notably, 84% valued WhatsApp messages highly in daily communication, yet 25.5% fell victim to phishing via WhatsApp, compromising their login details. These findings emphasize the urgent need for heightened cybersecurity awareness and education to mitigate risks and protect users from evolving cyber threats.

References

[1] AAG Phishing Statistics 2023 (updated December 2023). Retrived december 2023, https://aag-it.com/the-latest-phishing-statistics/

[2] Adrian Andrade (2023). Benchmark-Social Engineering. Grand Canyon University

[3] Young Choi (2023). Social Engineering Cyber Threats. Journal of Global Awareness. 4. 1-12. 10.24073/jga/4/02/08.

[4] Kaspersky. What is Social Engineering? Retrieved from: https://www.kaspersky.com/resce-center/definitions/what-is-social-engineering

[5] Cynthia Ignatius. (2022). Malaysia Remains Top Country In SEA When It Comes To Financial Phishing. Retrieved from: https://www.businesstoday.com.my/2022/11/01/malaysia-remains-top-country-in-sea-when-it-comes-to-financial-phishing/

[6] Reddy, Venkata Siva sankara (2019). Ethical Hacking Using Phishing attack Based on the Data Mining Technique.

[7] Tabassum, Mujahid & Sharma, Tripti & Mohanan, Saju. (2021). Ethical Hacking and Penetrate Testing using Kali and Metasploit Framework. International Journal of Innovation in Computational Science and Engineering Vol 2 No1, pp:09-22.

[8] R. S. Devi and M. M. Kumar (2020). Testing for Security Weakness of Web Applications using Ethical Hacking," 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), pp. 354-361,

[9] M. Lehrfeld and P. Guest (2016). Building an ethical hacking site for learning and student engagement, SoutheastCon 2016, 2016, pp. 1-6, doi: 10.1109/SECON.2016.7506746

[10] Publication, E. R., & I. J. E. A. S. (2014). International Journal of Modern Communication Technologies & Research (Vol. 2 Issue 5) May -2014. Engineering Research Publication .

[11] Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2016). Breaching the human firewall: Social engineering in phishing and spear-phishing emails. *arXiv preprint arXiv:1606.00887*.

979-8-3503-7303-5/24/$31.00 ©2024 IEEE

[12] Musuva, P., Chepken, C., & Getao, K. (2019). A naturalistic methodology for assessing susceptibility to social engineering through phishing. *The African Journal of Information Systems*, *11*(3), 2.

[13] Albladi, S. M., & Weir, G. R. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*, *8*(1), 1-24.

[14] Nicholson, J., Coventry, L., & Briggs, P. (2017). Can we fight social engineering attacks by social means. *Assessing social salience as a means to improve phish detection, SOUPS*.

[15] Halevi, T., Memon, N., & Nov, O. (2015). Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks*.

[16] Gupta, A. K., Srivastava, A., Goyal, T. K., & Saxena, P. (2014). ETHICAL HACKING: An Approach towards Penetration Testing. International Journal of Modern Communication Technologies and Research, 2(5), 265

979-8-3503-7303-5/24/$31.00 ©2024 IEEE