International Journal of Advances in Applied Sciences (IJAAS)
Vol. 13, No. 4, December 2024, pp. 882~890
ISSN: 2252-8814, DOI: 10.11591/ijaas.v13.i4.pp882-890

User perceptions of artificial intelligence powered phishing attacks on Facebook's resilient infrastructure

JosephNg Poh Soon[1,2], Rou Qian Chan[2], Qian Hui Lee[2], Dick En Loke[2], Stevenson Ling Heng Chun[2], Phan Koo Yuen[3]

[1]Department of Computer Science, Institute of Computer Science and Digital Innovation, UCSI University, Kuala Lumpur, Malaysia
[2]Department of Network and Security, Faculty of Data Science and Information Technology, INTI International University, Kuala Lumpur, Malaysia
[3]Department of Computer Science, Faculty of Information and Communication Technology, Universiti Tunku Abdul Rahman, Perak, Malaysia

Article Info

Article history:

Received Feb 19, 2024
Revised May 1, 2024
Accepted Jun 19, 2024

Keywords:

Cybersecurity
Inclusive innovation
Phishing attacks
Resilient infrastructure
Responsive institutions
Transparency monitoring tools

ABSTRACT

This study focuses on examining the user perceptions of a cybersecurity certificate transparency (CT) monitoring tool in the context of artificial intelligence (AI) powered phishing attacks on the Facebook platform. Implementing CT monitoring tools is one strategy for preventing these attacks. It reveals a significant level of concern among respondents regarding the potential risks associated with phishing attacks, indicating a growing awareness of the severity of such threats for future resilient infrastructure development. Users' knowledge and understanding of AI-driven phishing threats were found to vary, emphasizing the need for awareness campaigns towards sustainable development education. The study also highlights varying levels of confidence among users in effectively identifying and thwarting phishing efforts, suggesting the importance of user empowerment through improved training, tools, and technologies as responsive institutions. These findings underscore the significance of addressing user concerns, enhancing security awareness, and providing users with the necessary resources to protect themselves against sophisticated phishing attacks. The research contributes to the understanding of user perceptions and lays the groundwork for further improvements in security measures and user education in the fight against phishing threats on Facebook's inclusive growth.

Corresponding Author:

JosephNg Poh Soon
Department of Computer Science, Institute of Computer Science and Digital Innovation, UCSI University
Kuala Lumpur 56000, Malaysia
Email: joseph.ng@ucsiuniversity.edu.my

1. INTRODUCTION

Attackers and malicious actors have been using phishing as a security risk since the dawn of the Internet era [1]. Phishing is an attack where the malicious actor runs a fake website that looks like the real thing [2]. Sophisticated attackers use advanced artificial intelligence (AI) powered phishing tools to fool users into disclosing personal information by pretending to be somebody they know [1]. Facebook and other social media sites are particularly vulnerable to such attacks. Attackers might develop convincing fake profiles or messages that closely mimic those of a person the user knows and trusts, taking advantage of the enormous quantity of personal data readily available on these sites. This trickery seeks to make the user less vigilant and more likely to fall for the phishing scam. Users find it much harder to distinguish between legitimate and fraudulent emails due to the complexity and effectiveness added by the usage of AI

technology in phishing efforts. The security and privacy of online users are seriously threatened by phishing assaults. As social media sites like Facebook have grown in popularity, attackers are constantly devising new strategies to exploit vulnerabilities and deceive unsuspecting individuals. To counter these threats, various security measures have been implemented, including tools for monitoring certificate transparency (CT) [2]. This study aims to evaluate the effectiveness and perceptions of a specific CT monitoring tool in mitigating AI-powered phishing attacks on Facebook. Additionally, the study investigates the financial implications for affected individuals and organizations, as well as the long-term brand reputation repercussions for Facebook when its users' become targets of such attacks. Furthermore, the study aims to delve into the perceived concerns of Facebook users regarding AI-powered phishing attacks.

AI-powered phishing attacks often employ evasion tactics to bypass established security measures and evade detection. Phishing content can be subtly altered using adversarial machine learning algorithms, making it difficult for security systems to identify and prevent such attacks [3]. These tactics exploit vulnerabilities in security algorithms and systems, posing challenges in effectively detecting and mitigating AI-powered phishing attacks. AI algorithms can automatically generate phishing content, such as emails, texts, or social media posts that closely resemble legitimate communications from trusted sources. By learning patterns and linguistic characteristics from extensive datasets of real communications, these algorithms can create highly convincing phishing content that deceives unsuspecting individuals.

Spear phishing, a targeted form of phishing, aims to deceive specific groups or organizations. AI-driven spear phishing attacks utilize machine learning algorithms to gather and analyze large volumes of publicly available data about the target, including social media posts, professional profiles, or news articles [4]. Personalized phishing messages are then crafted based on this data, increasing the likelihood of successful deception. Additionally, AI algorithms can be employed to identify and analyze phishing kits, which are pre-assembled collections of tools and resources used by attackers to facilitate phishing campaigns. By leveraging machine learning techniques to identify patterns, signatures, and behavioral traits associated with phishing kits, security experts can more effectively detect and counteract phishing attempts. AI-powered phishing attacks frequently employ evasion tactics to circumvent established security measures and avoid detection. The subtle modifications made to phishing content using adversarial machine learning algorithms present challenges for security systems in accurately identifying and thwarting such attacks. The identification and prevention of AI-powered phishing attacks are further complicated by these tactics, capitalizing on weaknesses in security algorithms and systems.

A security protocol known as CT aims to enhance the reliability and security of digital certificates used for secure online communication by providing a transparent log of all issued certificates that is accessible to the public [4]. This enables early detection and mitigation of fraudulent or unauthorized certificates. Understanding the concept and implementation of CT is crucial in addressing certificate-related vulnerabilities and ensuring a more secure online environment. In a public key infrastructure (PKI), digital certificates serve as cryptographic artifacts that validate the integrity and authenticity of digital entities, such as servers, websites, and individuals. These certificates, issued by trusted certificate authorities (CAs), contain public keys, identity information, and other relevant data. However, managing certificates poses challenges and risks, including the issuance of unauthorized or fraudulent certificates due to errors or malicious actions by CAs, compromising the security and trustworthiness of online communications.

Nowadays, Facebook has become a ubiquitous social media platform that is extensively used in our daily lives. According to the article 'Malaysia Social Media Statistics and Facts 2023,' a staggering 83.8% of internet users in Malaysia utilize Facebook. This statistic highlights the significant role Facebook plays in our lives and underscores the potential impact of phishing attacks on this platform, which can be highly detrimental. Given the rapid advancements in AI technology, it begs the question: are we, as Facebook users, adequately prepared to defend against the increasingly sophisticated and elusive AI-powered phishing attacks that pose a significant threat to our security? While Facebook currently employs the CT monitoring tool to combat cyber-attacks, the effectiveness, and efficiency of this tool in detecting and preventing phishing attacks on the platform necessitates further examination. Therefore, the objective of this research is to provide insights into the effectiveness of the CT monitoring tool and propose enhanced solutions to bolster the prevention of AI-powered phishing attacks on Facebook. By doing so, we can strengthen the cybersecurity of Facebook users and ensure their safety while utilizing the platform. To visually depict the relationship between the hypotheses, a hypothesis research framework is presented in Figure 1 and Table 1. These elements collectively contribute to the structure and organization of the research, ensuring a systematic and coherent approach to the study. i) RH1: the implementation of the CT monitoring tool has had a positive impact on the defense against AI-powered phishing attacks on Facebook; ii) RH2: users' perception of Facebook's brand reputation is negatively affected when they fall victim to AI-powered phishing attacks; iii) RH3: AI-powered phishing attacks on Facebook hurt the financial well-being of individuals and organizations; and iv) RH4: Facebook users perceive AI-powered phishing attacks as a significant negative threat to their online security.

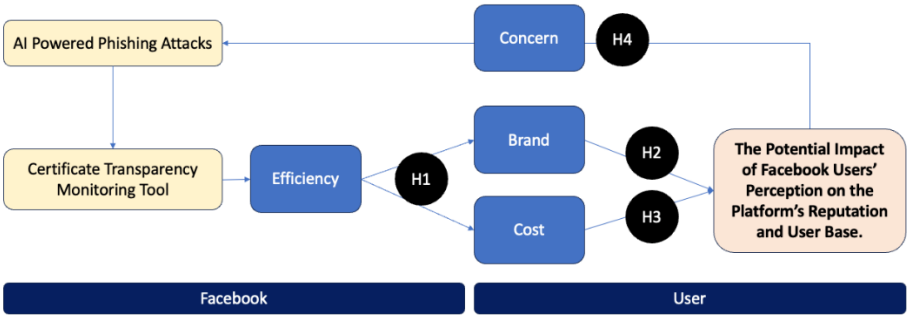

Figure 1. Hypothesis research framework

Table 1. AI tools and categorization targets

No	Tool	Target
1	Deepfake [5]	Facial image data [6]
2	uriDeep [1]	Textual data [7]
3	Voice generator [8]	Speech audio data [9]

AI can generate fabricated data and information through machine learning models. On the other end of the spectrum, in terms of traditional offensive cybersecurity measures, machine learning can be utilized to infiltrate networks and extract sensitive information that can be used to develop evasive malware and cause harm to systems it encounters. It can also be employed as a spear-phishing technique to gather information from specific individuals for various purposes [2]. Additionally, cybercriminals can manipulate machine learning algorithms by injecting flawed training data and modifying the model code, enabling them to evade detection and pursue their malicious objectives. The most concerning aspect is the use of advanced technology to remain undetected, as it can exhibit extreme persistence and pose a significant threat. Moreover, attackers may simultaneously launch a complex series of attacks targeting multiple individuals, using authentic voices through a combination of deepfake and voice generator attack methods. Thus, vishing closely resembles a spear-phishing attack.

Deepfakes, which involve the manipulation of audio, video, or image recordings using artificial intelligence techniques, produce realistic-looking fake content [3]. These manipulations utilize algorithms to replicate human speech, gestures, emotions, and facial expressions. Deepfakes are commonly used for entertainment purposes on social media platforms like Facebook and TikTok, often featuring impersonations of politicians, celebrities, and public figures. The potential harm caused by deepfakes is significant, as they can spread false information, damage reputations, and incite violence and instability, resembling sophisticated phishing attacks. Distinguishing between a deepfake and an authentic video of a person has become increasingly challenging for the general public.

In a recent incident, an AI-powered Reddit bot remained undetected for a week [4]. By generating comments using artificially generated data, the bot was able to convincingly pose as a human, fooling some individuals. This example highlights how such technology can be utilized to create and disseminate information that has the potential to incite conflicts within communities. Some researchers are even focusing on generating fake textual information to populate websites, which can be used to spread false news. Another concerning application involves duplicating the identities of personalities and social media influencers by creating mirror versions of their social media presence. Once the fraudulent account gains trust and appears legitimate, scammers can disseminate fake information and manipulate followers into investing in fraudulent cryptocurrencies. Furthermore, they may generate fake links to deceive users into providing personal information, such as birthdays, pet names, or street names, which are common security question prompts.

2. RESEARCH METHOD

This research study utilized a mixed-methods approach to comprehensively investigate user perceptions of the CT monitoring tool in mitigating AI-powered phishing attacks on Facebook. The methodology involved qualitative and quantitative data collection methods [5]–[7], [10]. The goal of the qualitative method is to get insight into consumers' current understanding of phishing attempts, their degree of confidence in Facebook, and their experiences with cybersecurity solutions. The quantitative method examines how users feel about the CT monitoring tool, including how simple they believe it to be to use, how reliable they believe its notifications to be, and how satisfied they are overall with

its functioning [8], [9], [11]–[13]. Qualitative insights were gathered through an open-ended survey questionnaire, allowing participants to share personal experiences, observations, and incidents related to AI-powered phishing attacks on Facebook. This qualitative data collection method enables a thorough exploration of user experiences and provides valuable context for understanding the impact of these attacks. Quantitative data was collected through a structured survey questionnaire consisting of 4 demographic questions and 16 technical questions [14]–[17] as shown in Figure 2. The technical questions included 12 Likert Scale 5 items measuring agreement levels and 4 open-ended questions for more detailed qualitative insights.

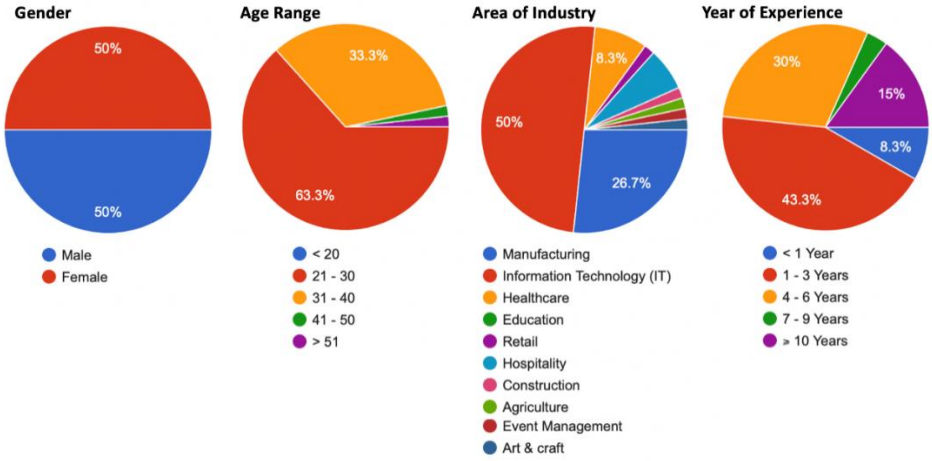

Figure 2. Demographics of respondents

3. RESULTS AND DISCUSSION

This study aimed to provide valuable insights into user perceptions of the CT monitoring tool in the context of AI-powered phishing attacks on Facebook. To achieve this goal, the research was organized into four distinct sessions, with Session I focusing on the effectiveness of the tool in preventing such attacks. A survey was conducted, and the findings revealed that the majority of respondents feel vulnerable to these attacks and have experienced them or know someone who has. Additionally, most respondents agreed that the tool is effective, although some remained neutral, indicating the need for further investigation.

Session I assessed the effectiveness of the CT monitoring tool in preventing AI-powered phishing attacks on Facebook. The research was organized into four sessions, with session I focusing on the effectiveness of the tool in preventing such attacks. A survey was conducted, and the findings revealed that most respondents feel vulnerable to these attacks and have experienced them or know someone who has. Additionally, most respondents agreed that the tool is effective, although some remained neutral, indicating the need for further investigation. The quantitative findings from the survey conducted in Session I are presented in Figure 3. The findings revealed that a majority of respondents (71.7%) feel vulnerable to these attacks, indicating significant concern among users. Additionally, 66.6% agreed or strongly agreed that they or someone they know has been a victim of AI-phishing attacks on Facebook. Regarding the effectiveness of the tool, 66.6% of respondents agreed or strongly agreed that it is effective, while 31.6% remained neutral, suggesting the need for further investigation. The qualitative analysis highlighted common experiences of encountering fake links, phishing posts, and scam calls on Facebook. Some respondents shared incidents where their friends' accounts were hacked, leading to the spreading of malicious content or phishing attempts.

Session II focused on analyzing the long-term brand reputation implications for Facebook in the face of AI-powered phishing attacks on users. The data analysis and discussion revealed insights from both quantitative and qualitative data. In terms of quantitative analysis (as shown in Figure 4), a majority of respondents (85%) agreed that if users fall victim to AI-powered phishing attacks on Facebook, it negatively impacts the brand reputation of the platform. Similarly, a significant majority (78.4%) agreed that users losing trust in Facebook due to such attacks can lead to a decline in the platform's user base. Additionally, 69.9% of respondents agreed that they would consider stopping using Facebook if they or someone they know became a victim of AI-powered phishing attacks. The qualitative analysis provided further insights into users' perspectives on why AI-powered phishing attacks on Facebook would lead them to stop using the platform. Common themes that emerged included concerns about financial losses, privacy, and data breaches, a lack of trust and feeling unsafe, and negative user experiences. The diagram likely shows data or

information that highlights the negative impact of AI-based phishing attacks on Facebook's customer base. Such attacks can result in the leaking of sensitive customer information, which could in turn drive users away from Facebook and towards other social media platforms that are perceived to be more secure.

Session III focused on understanding the financial implications of AI-powered phishing attacks on individuals and organizations in the context of Facebook. The quantitative analysis (as shown in Figure 5) revealed that a majority of respondents (65%) agreed that such attacks can lead to additional financial costs, including expenses for data recovery, investigations, and legal matters. Furthermore, 63.3% of participants agreed that AI-powered phishing attacks on Facebook can result in immediate losses and long-term consequences, such as damage to reputation and customer trust. It is worth noting that no respondents disagreed with this statement. When asked about the financial losses they had experienced, 23.3% reported no losses, while others indicated varying degrees of financial impact, with 20% suffering significant losses and 5% reporting severe losses. The qualitative analysis focused on mitigation measures, with respondents providing valuable suggestions. These recommendations encompassed technical strategies such as strengthening security measures through stronger passwords, multi-factor authentication (2FA), and enhanced account monitoring.

Session IV focused on exploring the perceived concerns of Facebook users regarding AI-powered phishing attacks. The quantitative findings from the survey conducted in session IV are presented in Figure 6. The survey results indicated varying levels of concern among participants, with the majority expressing some level of concern (86.7%). Of those, 30% were very concerned, and 16.7% were extremely concerned. In contrast, 13.3% indicated slight or no concern. Participants' confidence in identifying and avoiding AI-powered phishing attacks also varied, with 65% expressing moderate to high levels of confidence. However, 33.3% indicated lower levels of confidence, and 10% reported being not confident at all. The survey revealed a collective expectation (86.7% agreement) for Facebook to take stronger measures to protect users from these attacks. These findings underscore the need for continuous efforts to combat AI-powered phishing attacks on Facebook through user education, platform security enhancements, and proactive measures by the platform. The qualitative responses from users revealed the urgent need for Facebook to take proactive and continuous measures to combat the threat of AI-powered phishing attacks. One of these measures is to invest in user education programs that provide information on what phishing is, how it works, and how users can protect themselves from it.

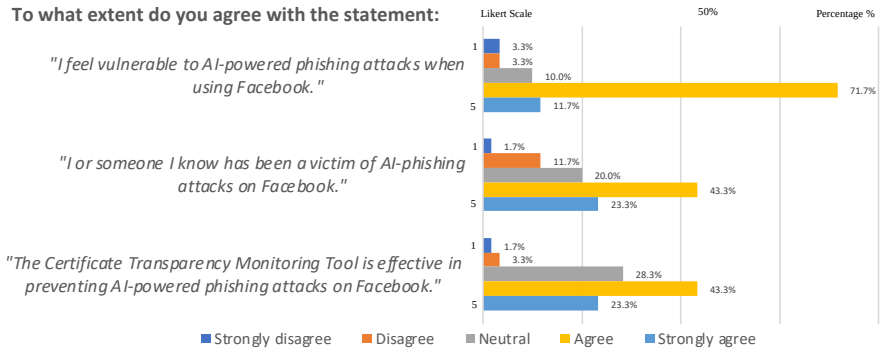

Figure 3. Quantitative findings from the survey conducted in session I

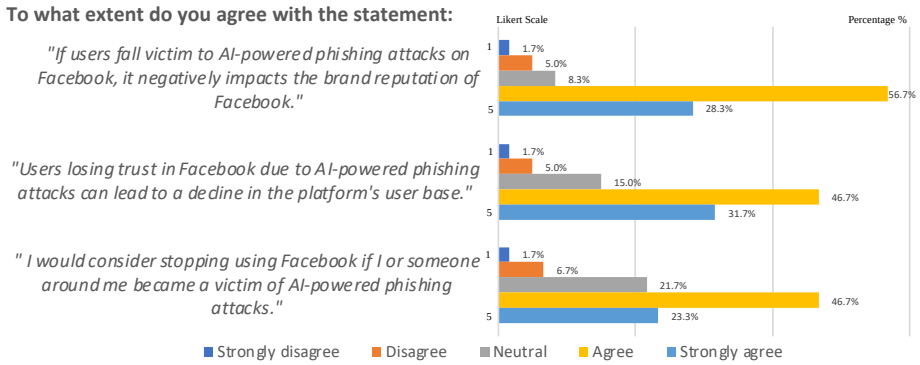

Figure 4. Quantitative findings from the survey conducted in session II

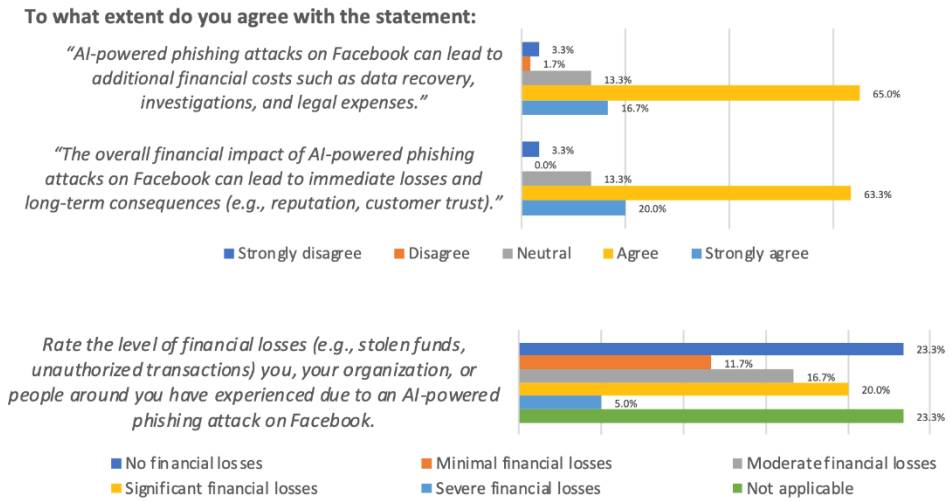

Figure 5. Quantitative findings from the survey conducted in session III

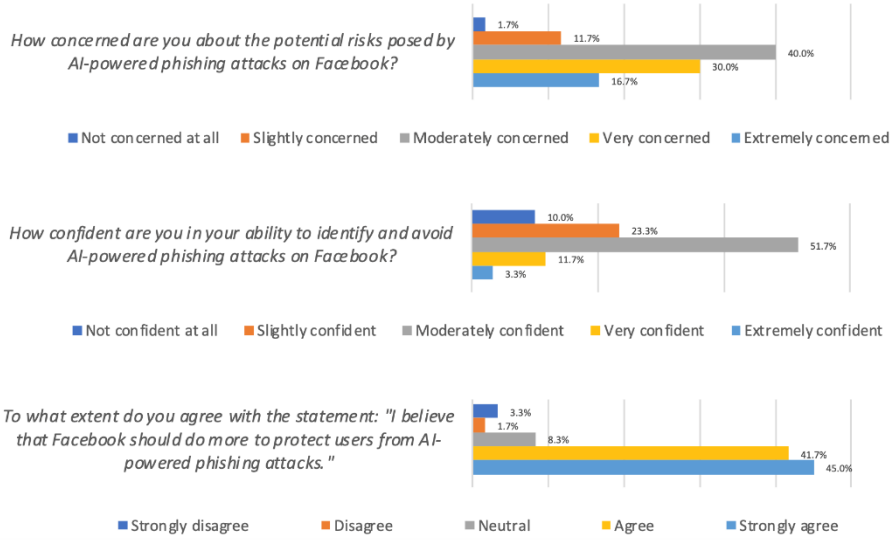

Figure 6. Quantitative findings from the survey conducted in session IV

This theoretical contribution extends our understanding of the effectiveness of CT monitoring tools in combating AI-powered phishing attacks, specifically in the context of a popular social media platform like Facebook. By examining user perceptions and experiences, this study sheds light on the importance of integrating advanced threat detection mechanisms, user education, and continuous research and development efforts to effectively combat AI-powered phishing attacks [18]–[20]. Moreover, the study identifies valuable recommendations, such as technical strategies, user education, collaboration with financial institutions, and implementing AI-based phishing detection algorithms [21]. These recommendations provide insights into the comprehensive approach required to enhance the defense against AI-powered phishing attacks on Facebook and create a safer online environment for users. However, the need for further investigation and validation of this tool is emphasized, which adds to the knowledge base regarding the effectiveness of AI-based security measures in combating phishing attacks. This research paper explores the societal contribution of addressing user concerns regarding AI-powered phishing attacks on Facebook. The study finds that these attacks pose a significant threat to user security, resulting in data breaches, financial losses, scams, and negative experiences [22], [23]. The research highlights the importance of privacy and user education in addressing these concerns and proposes strategies for enhancing cybersecurity measures and protecting users. The findings emphasize the potential for creating value and making a significant societal contribution through the development of

advanced threat detection and prevention mechanisms, ongoing research and development efforts, and user education and awareness initiatives. Implementing these multifaceted approaches fosters a safer online environment, contributing to the well-being and protection of individuals and organizations [24], [25]. The research serves as a valuable resource for policymakers, security professionals, and the broader community, ultimately aiming to create a more secure and resilient digital space for all. The study's societal contribution lies in promoting social, economic, environmental, or cultural progress and addressing the needs of communities, fostering a more inclusive, equitable, and sustainable future for society.

4. CONCLUSION

In conclusion, the examination of user perceptions of a CT monitoring tool in AI-powered phishing attacks on Facebook makes significant theoretical contributions to user education and awareness. By identifying specific areas where users lack understanding or hold misconceptions, targeted educational initiatives can be developed to address these gaps. Additionally, this research contributes to promoting responsible online behavior by understanding user perceptions of the risks associated with AI-powered phishing attacks. Strategies can then be developed to encourage safe practices and risk mitigation, foster a more secure online environment, and protect individuals from phishing attacks. Ultimately, the theoretical contributions derived from this research enhance user education and awareness, driving improvements in educational initiatives, user-friendly materials, and empowering strategies to safeguard against phishing attacks in the AI era. The goal is to create a more informed and resilient user base in the face of evolving online threats. The research paper proposes strategies for enhancing cybersecurity measures and protecting users, such as the use of CT monitoring tools, user education, collaboration with financial institutions, and the implementation of AI-based phishing detection algorithms. The study recognizes the long-term implications for Facebook's brand reputation resulting from AI-powered phishing attacks and the financial implications of such attacks. The research serves as a valuable resource for policymakers, security professionals, and the broader community, ultimately aiming to create a more secure and resilient digital space for all. The study's societal contribution lies in promoting social, economic, environmental, or cultural progress and addressing the needs of communities, fostering a more inclusive, equitable, and sustainable future for society.

REFERENCES

[1] M. M. Yamin, M. Ullah, H. Ullah, and B. Katt, "Weaponized ai for cyber attacks," *J. Inf. Secur. Appl.*, vol. 57, p. 102722, Mar. 2021, doi: 10.1016/j.jisa.2020.102722.

[2] E. Fasllija, H. F. Enişer, and B. Prünster, "Phish-hook: detecting phishing certificates using certificate transparency logs," in *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering ((LNICST,volume 305))*, Springer, Cham, 2019, pp. 320–334. doi: 10.1007/978-3-030-37231-6_18.

[3] A. Bhardwaj, V. Sapra, A. Kumar, N. Kumar, and S. Arthi, "Why is phishing still successful?," *Comput. Fraud Secur.*, vol. 2020, no. 9, pp. 15–19, Jan. 2020, doi: 10.1016/S1361-3723(20)30098-1.

[4] W. D. Heaven, "A gpt-3 bot posted comments on reddit for a week and no one noticed," MIT Technology Review. Accessed: Nov. 24, 2020. [Online]. Available: https://www.technologyreview.com/2020/10/08/1009845/a-gpt-3-bot-posted-comments-on-reddit-for-a-week-and-no-one-noticed/

[5] P. S. JosephNg, "Innovative usage of grid solutions with a technology behavior model in a medium-size enterprise," *Appl. Syst. Innov.*, vol. 6, no. 1, p. 11, Jan. 2023, doi: 10.3390/asi6010011.

[6] P. S. JosephNg, P. Sen BrandonChan, and K. Y. Phan, "Implementation of smart nfc door access system for hotel room," *Appl. Syst. Innov.*, vol. 6, no. 4, p. 67, Jul. 2023, doi: 10.3390/asi6040067.

[7] G. S. Al-Dharhani, Z. A. Othman, and A. A. Bakar, "A graph-based ant colony optimization for association rule mining," *Arab. J. Sci. Eng.*, vol. 39, no. 6, pp. 4651–4665, Jun. 2014, doi: 10.1007/s13369-014-1096-5.

[8] P. Kaur, F. Farahlina, A. Alam, S. Kaur, and R. S. Sahota, "Access control application prevention and mitigation of cyber attacks," *Int. J. Res. Innov. Appl. Sci.*, vol. 8, no. 10, pp. 91–105, 2023, doi: 10.51584/IJRIAS.2023.81011.

[9] P. S. JosephNg, "EaaS optimization: available yet hidden information technology infrastructure inside medium size enterprise," *Technol. Forecast. Soc. Change*, vol. 132, pp. 165–173, Jul. 2018, doi: 10.1016/j.techfore.2018.01.030.

[10] P. S. JosephNg, "Hotel room access control: an nfc approach ecotourism framework," *J. Sci. Technol. Policy Manag.*, vol. 15, no. 3, pp. 530–551, Apr. 2024, doi: 10.1108/JSTPM-10-2021-0153.

[11] T. Nandy, R. Md Noor, R. Kolandaisamy, M. Y. I. Idris, and S. Bhattacharyya, "A review of security attacks and intrusion detection in the vehicular networks," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 36, no. 2, p. 101945, Feb. 2024, doi: 10.1016/j.jksuci.2024.101945.

[12] T. Nandy *et al.*, "A secure, privacy-preserving, and lightweight authentication scheme for vanets," *IEEE Sens. J.*, vol. 21, no. 18, pp. 20998–21011, Sep. 2021, doi: 10.1109/JSEN.2021.3097172.

[13] N. K. Lung, P. L. Chong, and A. D. Deshinta, "Designing a research model for depression tendency detection using facial expression recognition," *J. Eng. Sci. Technol.*, vol. 19, no. 2, pp. 163–172, 2024, [Online]. Available: https://jestec.taylors.edu.my/Special Issue on ICIT2022_3/ICIT2022_3_18.pdf

[14] M. Huang and F. K. Chong, "Empowering travelers with airfare comparison, flight tracking, and real-time weather forecasts on android," in *2023 IEEE 11th Conference on Systems, Process & Control (ICSPC)*, IEEE, Dec. 2023, pp. 7–12. doi: 10.1109/ICSPC59664.2023.10420178.

[15] S. R. Sindiramutty *et al.*, "Modern smart cities and open research challenges and issues of explainable artificial intelligence," in *Advances in Explainable AI Applications for Smart Cities*, IGI Global, 2024, pp. 389–424. doi: 10.4018/978-1-6684-6361-1.ch015.
[16] L. H. Yong, K. Subaramaniam, A. S. Shibghatullah, and W. M. Wan Isa, "Design and development of gami-ccount: a gamified solution to increase undergraduates' learning engagement in the accounting subject," *Int. J. Eng. Trends Technol.*, vol. 71, no. 2, pp. 197–210, Feb. 2023, doi: 10.14445/22315381/IJETT-V71I2P223.
[17] M. Chen, A. S. Shibghatullah, K. Subramaniam, and X. Yang, "Weighted minimax programming subject to the max-min fuzzy relation inequalities," *AIMS Math.*, vol. 9, no. 6, pp. 13624–13641, 2024, doi: 10.3934/math.2024665.
[18] M. F. Ansari, "A quantitative study of risk scores and the effectiveness of ai-based cybersecurity awareness training programs," *Int. J. Smart Sens. Adhoc Network.*, vol. 3, no. 3, pp. 1–8, Mar. 2022, doi: 10.47893/IJSSAN.2022.1212.
[19] M. Shirvanian, M. Mohammed, N. Saxena, and S. A. Anand, "Voicefox: leveraging inbuilt transcription to enhance the security of machine-human speaker verification against voice synthesis attacks," in *Annual Computer Security Applications Conference*, New York, NY, USA: ACM, Dec. 2020, pp. 870–883. doi: 10.1145/3427228.3427289.
[20] J. B. Li, S. Qu, X. Li, J. Szurley, J. Z. Kolter, and F. Metze, "Adversarial music: real world audio adversary against wake-word detection system," *arXiv*, Oct. 2019, [Online]. Available: http://arxiv.org/abs/1911.00126
[21] M. F. Ansari, P. K. Sharma, and B. Dash, "Prevention of phishing attacks using ai-based cybersecurity awareness training," *Int. J. Smart Sens. Adhoc Network.*, pp. 61–72, Mar. 2022, doi: 10.47893/IJSSAN.2022.1221.
[22] S. Back and R. T. Guerette, "Cyber place management and crime prevention: the effectiveness of cybersecurity awareness training against phishing attacks," *J. Contemp. Crim. Justice*, vol. 37, no. 3, pp. 427–451, Aug. 2021, doi: 10.1177/10439862211001628.
[23] P. Tandon *et al.*, "Txt2Vid: ultra-low bitrate compression of talking-head videos via text," *arXiv*, Jun. 2021, [Online]. Available: http://arxiv.org/abs/2106.14014
[24] A. Drichel, V. Drury, J. von Brandt, and U. Meyer, "Finding phish in a haystack: a pipeline for phishing classification on certificate transparency logs," in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, New York, NY, USA: ACM, Aug. 2021, pp. 1–12. doi: 10.1145/3465481.3470111.
[25] J. A. Hall, "What we do in the shadows: the consumption of mobile messaging by social media mobile apps in the twilight of the social networking era," *Mob. Media Commun.*, vol. 11, no. 1, pp. 66–73, Jan. 2023, doi: 10.1177/20501579221133610.

BIOGRAPHIES OF AUTHORS

Prof. Ts. Dr. JosephNg Poh Soon graduated with a Doctor of Philosophy in Information Technology, Master in Information Technology (Aus), Master in Business Administration (Aus), and Associate Chartered Secretary (ICSA-UK) with various instructor qualifications, professional certifications, and industry memberships. Listed numerous times as the World's Top 2% Scientist in Artificial Intelligence and Image Processing by Stanford University, USA, and with his blended technocrat mix of both business senses and technical skills, has held many multinational corporation senior management positions, global posting and leads numerous 24x7 global mission-critical systems. He has appeared in LIVE national television prime time Cybersecurity talk shows and overseas teaching exposure. His current research is on strategic digital transformation. He can be contacted at email: joseph.ng@ucsiuniversity.edu.my.

Rou Qian Chan completed postgraduate studies at Department of Network and Security, Faculty of Data Science and Information Technology, INTI International University. Her research interests focus on the Network and Security, Data Science and Information Technology. She can be contacted at email: i22023453@student.newinti.edu.my.

Qian Hui Lee completed postgraduate studies at Department of Network and Security, Faculty of Data Science and Information Technology, INTI International University. Her research interests focus on the Network and Security, Data Science and Information Technology. She can be contacted at email: i18015310@student.newinti.edu.my.

Dick En Loke completed postgraduate studies at Department of Network and Security, Faculty of Data Science and Information Technology, INTI International University. His research interests focus on the Network and Security, Data Science and Information Technology. He can be contacted at email: i22023300@student.newinti.edu.my.

Stevenson Ling Heng Chun completed postgraduate studies at Department of Network and Security, Faculty of Data Science and Information Technology, INTI International University. His research interests focus on the Network and Security, Data Science and Information Technology. He can be contacted at email: i22023723@student.newinti.edu.my.

Asst Prof. Ts. Dr. Phan Koo Yuen graduated with a PhD in Business Information Technology (Malaysia) and an MSc in Information Studies (Singapore). He is currently working at the Department of Computer Science, Faculty of Information and Communication Technology, Universiti Tunku Abdul Rahman, Malaysia as a computer science assistant professor (Faculty of Information and Communication Technology). His research interests focus on the domains of information systems, information technology, business intelligence success, and firm performance. He can be contacted at email: phanky@utar.edu.my.