Information Sciences Letters

Volume 11
Issue 2 *Mar. 2022*

Article 10

2022

Reviewing Cybersecurity Awareness Training Tools Used to Address Phishing Attack at the Workplace

Mohammed Fahad Alghenaim
Advanced Informatics Department, Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, 54100, Kuala Lumpur, Malaysia, aalghenaim@graduate.utm.my

Nur Azaliah Abu Bakar
Advanced Informatics Department, Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, 54100, Kuala Lumpur, Malaysia, aalghenaim@graduate.utm.my

Fiza binti Abdul Rahim
Advanced Informatics Department, Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, 54100, Kuala Lumpur, Malaysia, aalghenaim@graduate.utm.my

Inf. Sci. Lett. **11**, No. 2, 391- 398 (2022)

Information Sciences Letters
An International Journal

http://dx.doi.org/10.18576/isl/110210

Reviewing Cybersecurity Awareness Training Tools Used to Address Phishing Attack at the Workplace

Mohammed Fahad Alghenaim [*], *Nur Azaliah Abu Bakar and Fiza binti Abdul Rahim*

Advanced Informatics Department, Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, 54100, Kuala Lumpur, Malaysia

Received: 1 Nov. 2021, Revised: 2 Jan. 2022, Accepted: 16 Jan. 2022.
Publishedonline:1 Mar. 2022.

Abstract: Public sector data and sensitive information are a prime target for cyberattacks. There are numerous popular security tools used across the globe to achieve automated network protection. This study reviews the following tools within the current study: KnowBe4, PhishingBox, PhishInsight, PhishThreat, PhishMe, and Gophish. The rationale behind the detailed review is comparing and contrasting various cybersecurity awareness training tools used to address phishing attacks at the workplace. The selected tools can be used as assessment or enhancement awareness tools; this depends on each tool's settings and system due to its integrated models and flexibility. Furthermore, social engineering attacks are recurrently evolving, so different security tools' strengths and weaknesses could help pick the right instrument for spotting and responding to digital attacks. As a result, this study discusses the drawbacks of the selected tools that can guide developers and services providers in improving the existing phishing awareness tools.

Keywords: Cybersecurity, Phishing, Public sector, workplace

1 Introduction

Even though social engineering attackers are always coming up with new tactics, the most popular method right now is to trick people into giving away their private information without even realizing they've been tricked by an attacker [1]. Social engineering attacks include stealing individual account information beaching complete networks, leading to unexpected, costly consequences. In both cases, Phishing, the most popular form of social engineering attack, uses all necessary tools to gain access to information or take control of the victim's computer [2]. According to [3], Phishing is used to investigate the least resistant path by fooling victims instead of openly attacking them.

The public sector is a primary target for attackers due to its sensitivity and valuable data [4]. Officials in the public sector have implemented numerous tools to enhance employees' awareness of phishing threats. According to [5], the growing number of co-working spaces shows a need for new technologies to continue to expand. Still, the problem in the public sector is that acquiring talented employees remains an omnipresent obstacle. This issue is apparent in the public sector regarding its exposure to phishing threats; it is pressing to enhance employees' awareness by training them with a unique method regarding these threats and related subjects. Many employees in the public sector do not realize they are exposed to phishing threats, which means it is essential to intensify the awareness-enhancement process in the public sector to counter these threats [6]. Although phishing attacks represent a general threat in the public sector that needs to be countered, some institutions (e.g., ministries, public services, and educational and health institutions) are the primary targets for such attacks.

Realizing this issue, there is a necessity to improve the existing phishing awareness tools that can address the phishing attack at the workplace and at the same time be able to turn it into a cybersecurity training input, especially thru digital learning platform. To achieve this aim, this study has reviewed cybersecurity awareness training tools used to address phishing attacks at the workplace. The remainder of this paper is organized as follows: Section 2 introduces the different cybersecurity awareness training tools. Section 3 compares components services of awareness training tools. Section 4 discusses the drawbacks of cybersecurity awareness training tools. Finally, the conclusion is presented in Section 4.

2 Cybersecurity Awareness Training Tools

2.1 KnowBe4

As a security awareness training instrument, KnowB4 is advantageous because it focuses on developing and customizing existing approaches to Phishing and other social engineering threats. This tool functions based on an integrated platform that allows for more accessible simulated

*Corresponding author e-mail: aalghenaim@graduate.utm.my

training and the possibility of keeping all functions in one place [6]. In the literature, this particular framework is known as 'random attack deliveries' required to improve the rate of realism characteristic of messages shared by KnowB4 or any other awareness training instrument [7]. Paired with the exceptional quality of messages shared via KnowB4, it may also be safe to say that random attack delivery is a beneficial method of checking in with employees and the process of implementing new security features. This framework also suggests that the system generates timely reports to increase employee and threat visibility and strengthen phishing simulation [8].

The ultimate section of the framework characteristic of KnowB4 is the developers' willingness to implement new risk evaluation points and keep the score depending on the proposed awareness and training plan and the number of threats identified within the system. The system has thirteen modules, as shown in Table 1.

Table 1. Percentages of solutions for sample preparation

Module	Code
Add a recipient	A1
Select recipients	A2
Set a schedule	A3
Send To	A4
Track activity	A5
Categories	A6
Difficulty Rating	A7
Phish Link Domain	A8
Add Exploit	A9
Add Clickers To	B1
Email Templates	E1
Landing Pages	L1
Reports	R1

2.2 PhishingBox

The key to the functions of PhishingBox is the presence of a dedicated training sever that every authorized end-user could exploit to keep their productivity at a high level and minimize disruptions by any means [9]. Greene et al. (2018) [10] and Jampen et al. (2020) [11] suggest that similar employee training is crucial to digital security because it identifies the biggest threats and ensures they do not fall for the future. Compared to KnowB4, PhishingBox relies on real-time operations and reporting, as security must be addressed as a dynamic concept. The developers of PhishingBox offer a fully-fledged phishing simulator that could help the team monitor the team's progress in identifying and approaching social engineering threats [12].

Based on the available functions and specifications, it may also be claimed that PhishingBox can streamline the security process with targeted measures. With a significant amount of additional content available from a specialized library updated on time, the developers' focus on real-time protection pays off majorly [13]. The opportunity to set up custom courses for employees is another vital feature of PhishingBox that is not usually found in similar applications. The program's logic also requires repeated testing, which is advantageous because administrators target their efforts beyond mere attack simulations. However, the system has eight modules, as shown in Table 2.

Table 2. PhishingBox main modules used in the awareness tool

Module	Code
Add a recipient	A1
Select recipients	A2
Set a schedule	A3
Enrolled	C1
Not started	C2
In progress	C3
Completed	C4
Reports	R1

2.3 PhishInsight

The key feature behind the success of PhishInsight is the presence of an extensive template library that allows app administrators to generate custom emails for employees [14]. In the literature, such customization is addressed as an opportunity to set up beneficial training programs with rewards and real-life conditions that can be replicated if necessary [15]. The user can create awareness training and awareness simulation to enhance the users' awareness of phishing attacks. The crucial feature of PhishInsight is that it tracks all the data regarding interactions with mock phishing operations and provides the team with a better understanding of what areas of the organizational network could be addressed to improve their response to digital threats. This may also be met in the literature under visualization dashboards that stand for accurate data presentation and numerous filters for data analysis [16].

Like other instruments on the list, PhishInsight can be rightfully customized to become an incredibly realistic simulation of spear-phishing or any other type of Phishing. Each campaign created with the help of PhishInsight follows the strict rules of customization and real-world environments that contribute to the phish-assess-improve-phish cycle. The system has seven modules, as shown in Table 3.

Table 3. PhishInsight main modules used in the awareness tool

Module	Code

Add a recipient	A1
Select recipients	A2
Set a schedule	A3
Training Modules	Z1
Select a sender	C1
Select a Template	C2
Reports	R1

2.4 PhishThreat

The PhishThreat app's framework mainly focuses on creating campaigns intended to improve the team's awareness factor on a long-term scale [17]. PhishThreat is much closer to an accurate campaign and useful knowledge sharing than other applications from the list than its competitors[17]. This becomes possible owing to the synchronized security measures that serve as the basis of this app's operations [18]. The team gets a chance to create risk profiles for every user in the system and their respective actions, allowing for a targeted simulation to predict future attacks. The tool can send a testing Phishing assessing mails, providing clicking malicious links, opening malicious attachments, and supplying funds or data [17]. The PhishThreat app is also relatively substantial because it engages all employees in the simulation process instead of pointing to individual team members [19].

Overall, this is the most diminutive risky instrument on the list because its framework is based on real-time operations and feedback, leading to quicker identification of attackers and victims. The reporting process is also relatively intuitive, making targeted simulations aimed at risky behaviours a definite asset for the organization exploiting PhishThreat. This approach distantly resembles traditional training procedures, which may also be beneficial for the organization, as synchronized security would help the executives quickly point out all the employees who disregard security awareness as a whole [20]. The tool has an advanced dashboard with dynamic reports. In addition, the system covers nine (9) modules, as shown in Table 4.

Table 4. PhishThreat main modules used in the awareness tool

Module	Code
Add a recipient	A1
Select recipients	A2
Domain Spoofing	A8
Whitelist or IPs	Z2
Training Modules	Z1
Create a campaign/Send to	A4
Reports	R1
View Attacks	V1
View Training	V2

2.5 PhishMe

The PhishMe module is based on two digital protection layers: employee awareness and gateway strength, respectively [21]. The program helps the team identify the weakest spots across the network and assess the potential to mitigate these challenges [22]. According to Yang et al. (2019) [23], this reliance on digital intelligence is crucial because it quickly points to the solutions that can be integrated easily, without additional campaigns and irrelevant resource allocation.

As soon as the program verifies the network's suspicious area, it generates a unique response intended to remain in line with the network's needs and the company's policy on cybersecurity [24]. What significantly sets PhishMe apart from other solutions on the list is a security center serving as a chat room for security experts and businesses looking for help.

In a way, simulations and reports offered by PhishMe could become a perfect opportunity for employees to gain more insight into cybersecurity threats and get to educating others on the topic of social engineering [25]. However, PhishMe developers' framework suggests that mere awareness training initiatives are insufficient to cover workers' lack of specialized knowledge. This scenario makes it reasonable to install this software when the team does not have enough relevant experience and lacks an all-inclusive approach to social engineering. In addition, the system covers ten (10) modules, shown in Table 5.

Table 5. PhishMe main modules used in the awareness tool

Module	Code
Add a recipient	A1
Select recipients	A2
Send to	A4
Track activity	A5
Categories	A6
In progress	C3
Completed	C4
Select a sender	C5
Email Templates	E1
Reports	R1

2.6 Gophish

Another important InfoSec tool is available online named, GoPhish [26]. This tool is different from previous tools in that it provides an open-source tool to be used and upgraded

regarding any requirements the adopter wants. Gophish is an easy-to-use, powerful, and easily available open-source framework that enables companies to simulate, identify and rectify email phishing attacks to their network, as shown in Figure 1.

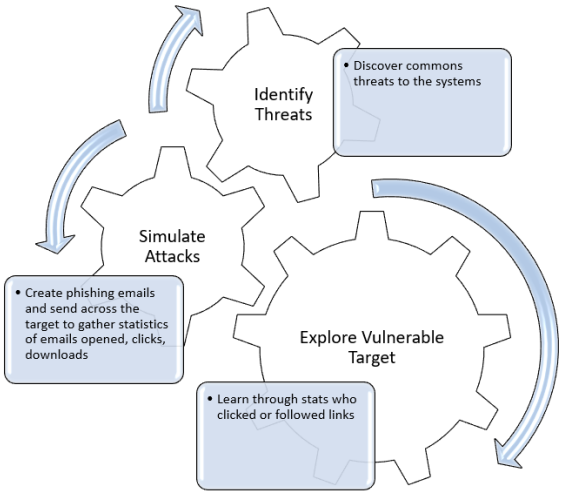

Figure 1. Gophish flow mechanism

The main idea behind the framework is to provide an industry-level phishing simulation tool that can run across platforms such as Linux, Windows, and MAC OSX. Phishing attack simulators focus on intelligently identifying threats, vulnerable access points, and the organization's overall behaviour. Gophish framework has been written in "Go" programming language that simplifies building from source with just the language editor and a C compiler. Moreover, Gophish was built with JSON API, enabling developers and system administrators to create custom phishing companions easily [25]. Installing Gophish is just as simple as downloading the zip file and installing it according to the platform. The product documentation covers all the configuration information relevant to each platform; to execute the tool and create the campaign, the employees or recipients of the campaign should access the phishing server. The system admin must make sure that the IP address of the phishing server is reachable from the LAN. According to research by Symantec, among 200 emails, every fourth email was identified as a Phishing email. As shown in Figure 2, the study found that 96% of Phishing attacks are delivered through email with commonly trusted file attachments (*.doc, *.pdf).

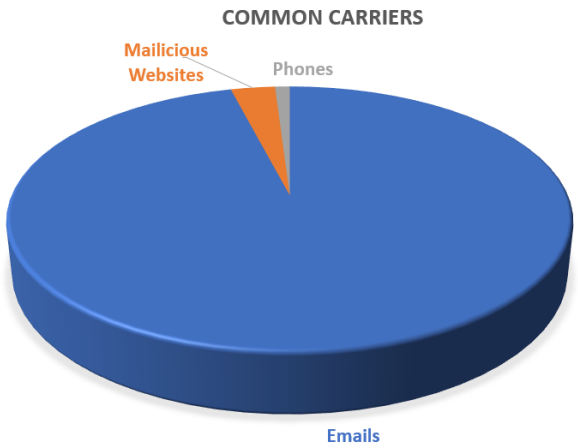

Figure 2. Phishing attacks common carriers

This suggests that email servers and communication is the most vulnerable target in organizations. Gophish enables the creation of campaigns within the organization with recipients in-house or remote, enabling monitoring of the landing pages and profiles. These campaigns are targeted explicitly towards email-based Phishing attacks. Along with tracking the attacking threat, vulnerable areas of the network, and identifying any loopholes in securing sensitive information, the tool can also help train the employees across the network to identify the threats and report accordingly [27]. The following figure shows the simple and comprehensive monitoring of a campaign in Gophish. The chart shows the various phishing attacks [28].

The statistics of a campaign show the behaviour of employees when receiving a Phishing email, enabling the system admins to profile the users and use this data to train and educate the employees. This tool is a complete framework and safe and can be used locally in any Saudi public sector because the institution's developers can modify it according to the InfoSec department's needs. However, it does not support embedding the phishing-related security policies to be tested by the user.

3 Comparing Components Services of Awareness Training Tools

This study has compared the provided online information security awareness tools based on the two factors; enhancing employees' ability to counter email phishing attacks and enhancing employees about related security policies, as shown below in Table 6.

Table 6. Comparison based on phishing types of attacks and security policies

Factor / Tool	Enhancing employees' ability to counter Phishing types attacks	Enhancing employees about related security policies
KnowBe4	√	☒
Phishing Box	√	☒
Phish Insight	√	☒
Phish Threat	√	☒
PhishMe	√	☒
Gophish	√	☒

The study shows each tool's main modules and components to build a matrix table to clarify the similarities and differences regarding the services provided, as shown in Table 7.

Table 7. The tools' components matrix

Modules / Components / Tool	Add a recipient	Select recipients	Set a schedule	Create a campaign/Send	Track activity	Categories	Difficulty Rating	Phish Link Domain	Add Exploit	Add Clickers To	Enrolled	Not started	In progress	Completed	Select a sender	Email Templates	Landing Pages	Reports	Training Modules	View Attacks	View Training	Whitelist or IPs
Code	A1	A2	A3	A4	A5	A6	A7	A8	A9	B1	C1	C2	C3	C4	C5	E1	L1	R1	Z1	V1	V2	Z2
KnowBe4	√	√	√	√	√	√	√	√	√	√	☒	☒	☒	☒	☒	√	√	√	☒	☒	☒	☒
PhishingBox	√	√	√	☒	☒	☒	☒	☒	☒	☒	√	√	√	√	☒	☒	☒	√	☒	☒	☒	☒
PhishInsight	√	√	√	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	√	√	☒	√	√	☒	☒	☒
PhishThreat	√	√	☒	√	☒	☒	☒	√	☒	☒	☒	☒	☒	☒	☒	☒	☒	√	√	√	√	√
PhishMe	√	√	☒	√	√	√	☒	☒	☒	☒	☒	☒	√	√	√	√	☒	√	☒	☒	☒	☒
Gophish	√ It is an open-source tool that can be upgraded to meet all InfoSec needs regarding Phishing attacks training																					

4 Drawbacks of Cybersecurity Awareness Training Tool

Although these online awareness tools have many advantages in enhancing the employees' awareness of phishing attacks, they still have severe drawbacks related to their scope and other security issues. First, foreign companies and organizations own these tools. An additional problem many organizations underestimate when exploring phishing threat awareness solutions is the high prevalence of foreign instruments. The idea is that they are built differently and may not be aligned against the existing political or economic situation within an organization (Bullée et al., 2018). This also means that the logic behind definite network security activities could differ based on the common human decisions made within a specific environment, as judgment operations and techniques rely on personal characteristics or cultural variations. Simply put, the existence of bias and foreign regulations could limit an instrument's use, creating dangerous scenarios where employees would not have a chance to increase their awareness due to not understanding what is expected (Juncos, 2017). Unfortunately, Phishing attack prevention software cannot cope with such differences and provide the team with solid advantages.

In addition, foreign organizations' involvement represents a threat because most security systems are built to underestimate attacker abilities and emphasize the learning process. Suppose a European developer and a US-based organization agree to a social awareness training application. In that case, Western peers could witness their expectations not being met because of the differences in approaches to social engineering threats. While the applications made by the US programmers are quickly overcoming this flaw by including as many preventive techniques as possible, their European counterparts seem to lag behind quite a bit because of the lack of knowledge regarding the context of social engineering attacks and their subjective nature [27].

Albladi and Weir (2018) [29], stated that even a strong vision makes it easier for developers to market their product and deploy it while considering any potential end-user's unique characteristics. Finally, it is a high risk to use any foreign awareness tool because they assess the current employees' awareness in the Saudi public sector and discover their weaknesses using these tools as reconnaissance weapons. Security agents or foreign governments could own these tools to spy on the customers and understand their weakest points [30]. In addition, these companies can sell the information they have regarding the weakness, security

reports to the foreign governments to gain money and give the advantage to these foreign governments to lunch Phishing attacks against the Saudi public sector.

Second, these tools do not cover the related security policies of phishing attacks, which is another crucial point that cannot be ignored is the challenge of the inability to test employee knowledge of the newly instilled security policies. Despite the strength of awareness-building applications, they rarely come with the functionality of testing workers' knowledge [31]. This scenario can be a disadvantage because most Phishing awareness training applications provide employees with all the necessary information about such attacks but fail to enhance the awareness regarding the related security policies. In other words, most phishing awareness training sessions are activities that get workers acquainted with the threat and help them identify the most common Phishing threats but never follow up with a knowledge test or any other means of validating the knowledge [24].

This is a serious drawback for any organization that cannot be overlooked or mediated quickly. Security policies make up for a crucial element of organizational protection within the existing digital space. It may be reasonable to claim that Phishing awareness cannot be achieved without a prolonged series of training and employee examinations to highlight the weakest and the strongest spots among all workforce members [32]. When discussing phishing awareness training tools, one should point out the lack of accessible options to protect the organization from digital attacks. The problem with most security policies is that they are outlined in a complex manner that averts employees from paying proper attention to securing the network by testing their knowledge [31]. According to Howard and Gutworth (2020) [33], workers quickly change their attitudes toward phishing threats after the training and start perceiving them much more frivolously instead of vigilance.

Third, these tools use the Internet to deliver their services to customers. The biggest problem out of all three is that most phishing awareness training tools have access to the Internet to remain reliable and efficient. Without real-time simulations, any given tech instrument becomes a mere toy in the hands of an organization, depreciating its value and reducing the effectiveness of training [34]. The lack of direct access to required instruments damages one's ability to coordinate activities and distinguish the most evident social engineering attacks. Security risks are relatively high when devices are not connected to the Internet, but the magnitude increases even more when at least one device gets connected [35].

This puts a strain on the organization because most business operations cannot be completed without a stable Internet connection. Even the slightest signal interruption could become a cornerstone of a data breach. This interdependency makes it harder for the management to plan activities or improve employee access to learning materials. The need to synchronize everything makes it safe to say that such information systems would not survive without the Internet [36]. Accordingly, hackers could damage an unprotected network with their bare hands, not even applying any digital tools pressure. Phishing requires an exquisite level of attention, and there has to be an opportunity to transfer at least some preventive techniques to the offline field [1].

Awareness training should go beyond digital instruments that use the Internet and be included in the local networking (internal link), including the employees' awareness discussions group. The need to remain connected to the Internet is a crucial security gap that averts many organizations from improving their operations and gives the attackers a chance to lunch Phishing attacks. Therefore, there is a need to use the VPN protocol to secure the internet connection when using the online training when using the proposed tool outside the institution from a distance.

Fourth and last, many anti-phishing tools are insufficient in detecting all Phishing attacking types. Therefore, anti-phishing tools cannot solve problems related to the human element and ignore their fallibility in decision-making ability because they do not consider the user's self-confidence an essential element. People, no doubt are ", susceptible to make poor trust decisions online." These problems are due to the limitation in adopting conceptual and procedural knowledge about Phishing attacks [37]. According to Misra et al. (2017), "automated tools have largely failed to mitigate phishing attacks, and even the best anti-phishing tools have been found to miss over 20% of phishing websites" [37].

5 Conclusions

There are many different threat types related to phishing attacks. Moreover, the public sector's natural culture is different in its assets, data, and value from the private sector. Without understanding and being aware of missing factors, components, and the related security policies implemented in the environment, focusing only on phishing attacks, in general, cannot prevent the public sector from being vulnerable to attacks.

Despite the numerous advantages and their acknowledged effectiveness, the cybersecurity awareness training tools possess some drawbacks as listed below:

- These awareness tools are owned by foreign organizations and companies mostly;
- These awareness tools are limited only to some phishing attacks;
- They fail to address the security standards and policies relating to phishing threats;
- Automated and anti-phishing tools have largely failed to enhance users' awareness of phishing attacking types;
- They rely on the Internet to provide awareness services that may not be accessible for everyone and pose the users to risks; and
- Even the open-source tool, such as Gophish, is limited to only phishing attacks technical training and cannot test the employees' awareness regarding

related security policies because this point requires much changing in the tool's structure itself.

As a result, a severe need to formulate a conceptual awareness model with all necessary factors and components to fit with the public sector needs in enhancing their employees' awareness of phishing attacks. Indeed, the literature review shows that these tools need to be upgraded by formulating a conceptual awareness model that can work in the workplace and e-learning with a practical awareness tool to avoid any lack of training regarding any future pandemic.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this article.

References

[1] P. Vadrevu and R. Perdisci, "What you see is not what you get: Discovering and tracking social engineering attack campaigns," in *Proceedings of the Internet Measurement Conference*, pp. 308–321, 2019.

[2] F. Salahdine and N. Kaabouch, "Social Engineering Attacks: A Survey. Future Internet, 11, 89." 2019.

[3] A. Rege, T. Nguyen, and R. Bleiman, "A social engineering awareness and training workshop for STEM students and practitioners," in *2020 IEEE Integrated STEM Education Conference (ISEC)*, pp. 1–6, 2020.

[4] S. M. Albladi and G. R. S. Weir, "Predicting individuals' vulnerability to social engineering in social networks," *Cybersecurity*, vol. 3, no. 1, p. 7, 2020.

[5] K. A. Siddiqui, M. E. Al-Shaikh, I. A. Bajwa, and O. Alenzi, "Venture capital challenges in Saudi Arabia," *Entrep. Sustain. Issues*, vol. 8, no. 3, p. 291, 2021.

[6] A. Suleimanov, M. Abramov, and A. Tulupyev, "Modelling of the social engineering attacks based on social graph of employees communications analysis," in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, pp. 801–805, 2018.

[7] R. Heartfield, G. Loukas, and D. Gan, "An eye for deception: A case study in utilizing the human-as-a-security-sensor paradigm to detect zero-day semantic social engineering attacks," in *2017 IEEE 15th international conference on software engineering research, management and applications (SERA)*, pp. 371–378, 2017.

[8] R. Taib, K. Yu, S. Berkovsky, M. Wiggins, and P. Bayl-Smith, "Social engineering and organisational dependencies in phishing attacks," in *IFIP Conference on Human-Computer Interaction*, pp. 564–584, 2019.

[9] Phishingbox, "Phishing Simulation & Awareness Training," 2021. [Online]. Available: https://www.phishingbox.com. [Accessed: 05-Nov-2021].

[10] K. Greene, M. Steves, and M. Theofanos, "No phishing beyond this point," *Computer (Long. Beach. Calif).*, vol. 51, no. 6, pp. 86–89, 2018.

[11] D. Jampen, G. Gür, T. Sutter, and B. Tellenbach, "Don't click: towards an effective anti-phishing training. A comparative literature review," *Human-centric Comput. Inf. Sci.*, vol. 10, no. 1, pp. 1–41, 2020.

[12] E. J. Williams, J. Hinds, and A. N. Joinson, "Exploring susceptibility to phishing in the workplace," *Int. J. Hum. Comput. Stud.*, vol. 120, pp. 1–13, 2018.

[13] F. Kolini, H. Shahbaznezhad, and M. Rashidirad, "An investigation into the factors influencing employees' behavior in phishing attacks," 2020.

[14] Trend Micro, "Phish Insight. Retrieved," 2021. [Online]. Available: https://phishinsight.trendmicro.com/en/. [Accessed: 05-Nov-2021].

[15] A. Oest, Y. Safei, A. Doupé, G.-J. Ahn, B. Wardman, and G. Warner, "Inside a phisher's mind: Understanding the anti-phishing ecosystem through phishing kit analysis," in *2018 APWG Symposium on Electronic Crime Research (eCrime)*, pp. 1–12, 2018.

[16] M. Mossano, K. Vaniea, L. Aldag, R. Düzgün, P. Mayer, and M. Volkamer, "Analysis of publicly available anti-phishing webpages: contradicting information, lack of concrete advice and very narrow attack vector," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 130–139, 2020.

[17] Sophos, "Sophos Phish Threat," 2019. [Online]. Available: https://www.sophos.com/en-us/medialibrary/pdfs/factsheets/sophos-phish-threat-datasheet.pdf. [Accessed: 11-Nov-2021].

[18] P. Peng, L. Yang, L. Song, and G. Wang, "Opening the blackbox of virustotal: Analyzing online phishing scan engines," in *Proceedings of the Internet Measurement Conference*, pp. 478–485, 2019.

[19] J. Mao, W. Tian, P. Li, T. Wei, and Z. Liang, "Phishing-alarm: robust and efficient phishing detection via page component similarity," *IEEE Access*, vol. 5, pp. 17020–17030, 2017.

[20] C. Pham, L. A. T. Nguyen, N. H. Tran, E.-N. Huh, and C. S. Hong, "Phishing-aware: a neuro-fuzzy approach for anti-phishing on fog networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 15, no. 3, pp. 1076–1089, 2018.

[21] Confense, "Phishing awareness training and threat simulations," 2021. [Online]. Available: https://cofense.com/product-services/phishme/. [Accessed: 01-Dec-2021].

[22] A. Zamir *et al.*, "Phishing web site detection using diverse machine learning algorithms," *Electron. Libr.*, 2020.

[23] P. Yang, G. Zhao, and P. Zeng, "Phishing website detection based on multidimensional features driven by deep learning," *IEEE Access*, vol. 7, pp. 15196–15209, 2019.

[24] M. J. A. Miranda, "Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach," *Int. Manag. Rev.*, vol. 14, no. 2, pp. 5–10, 2018.

[25] Z. Dou, I. Khalil, A. Khreishah, A. Al-Fuqaha, and M. Guizani, "Systematization of knowledge (sok): A

systematic review of software-based web phishing detection," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 4, pp. 2797–2819, 2017.

[26] Getgophish, "Documentation," 2021. [Online]. Available: https://getgophish.com/documentation/. [Accessed: 10-Dec-2021].

[27] J. Wallen, "How to run a phishing attack simulation with GoPhish," 2020. [Online]. Available: https://www.techrepublic.com/article/how-to-run-a-phishing-attack-simulation-with-gophish/. [Accessed: 15-Dec-2021].

[28] M. Rosenthal, "Must-Know Phishing Statistics: Updated 2021," 2021. [Online]. Available: www.tessian.com. [Accessed: 12-Dec-2021].

[29] S. M. Albladi and G. R. S. Weir, "User characteristics that influence judgment of social engineering attacks in social networks," *Human-centric Comput. Inf. Sci.*, vol. 8, no. 1, pp. 1–24, 2018.

[30] M. Bossetta, "The weaponization of social media: Spear phishing and cyberattacks on democracy," *J. Int. Aff.*, vol. 71, no. 1.5, pp. 97–106, 2018.

[31] H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues," *Futur. Internet*, vol. 11, no. 3, p. 73, 2019.

[32] I. Ghafir *et al.*, "Security threats to critical infrastructure: the human factor," *J. Supercomput.*, vol. 74, no. 10, pp. 4986–5002, 2018.

[33] M. C. Howard and M. B. Gutworth, "A meta-analysis of virtual reality training programs for social skill development," *Comput. Educ.*, vol. 144, p. 103707, 2020.

[34] A. Koyun and E. Al Janabi, "Social engineering attacks," *J. Multidiscip. Eng. Sci. Technol.*, vol. 4, no. 6, pp. 7533–7538, 2017.

[35] L. Xiangyu, L. Qiuyang, and S. Chandel, "Social engineering and insider threats," in *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pp. 25–34, 2017.

[36] A. E. Juncos, "Resilience as the new EU foreign policy paradigm: a pragmatist turn?," *Eur. Secur.*, vol. 26, no. 1, pp. 1–18, 2017.

[37] G. Misra, N. A. G. Arachchilage, and S. Berkovsky, "Phish phinder: a game design approach to enhance user confidence in mitigating phishing attacks," *arXiv Prepr. arXiv1710.06064*, 2017.