Anti-Phishing Awareness Delivery Methods

Abdulbasit Darem
Computer Science Department
Northern Border University
Arar, Saudi Arabia
basit.darem@nbu.edu.sa

Abstract-Phishing attacks are increasingly exploited by cybercriminals, they become more sophisticated and evade detection even by advanced technical countermeasures. With cybercriminals resorting to more sophisticated phishing techniques, strategies, and different channels such as social networks, phishing is becoming a hard problem to solve. Therefore, the main objective for any anti-phishing solution is to minimize phishing success and its consequences through complementary means to advanced technical countermeasures. Specifically, phishing threats cannot be controlled by technical controls alone, thus it is imperative to complement cybersecurity programs with cybersecurity awareness programs to successfully fight against phishing attacks. This paper provides a review of the delivery methods of cybersecurity training programs used to enhance personnel security awareness and behavior in terms of phishing threats. Although there are a wide variety of educational intervention methods against phishing, the differences between the cybersecurity awareness delivery methods are not always clear. To this end, we present a review of the most common methods of workforce cybersecurity training methods in order for them to be able to protect themselves from phishing threats.

Keywords-anti-phishing awareness; phishing; phishing attack; awareness delivery methods; cybersecurity threats

I. INTRODUCTION

Advances in technology have transformed the way people work, communicate, and socialize quite dramatically. This has also exposed people and companies to various threats, one of which is phishing. Phishing attacks form one of the most common cybersecurity threats that individuals and businesses face around the world, costing victims billions of dollars. Phishing is described as a potent attack vector by which cybercriminals gain access to networks and systems to deliver malicious payloads (e.g. ransomware) or siphon off valuable and sensitive information (e.g. login credentials for online banking or e-commerce sites) from potential victims. Phishing primarily depends on the perception of authenticity normally enacted through authentic-looking emails and spoofed websites purportedly from a legitimate and trusted source. It also masquerades hidden malicious payloads, such as ransomware, as authentic products or services. Figure 1 shows the unique fake websites and phishing emails detected by APWG just in the first quarter (Q1) of 2020, which are significantly higher than during the previous years [1]. Many fake websites are exact copies of the genuine websites, which make it difficult for people to recognize them as illegitimate websites. These malicious websites usually remain on-line for a short time only.

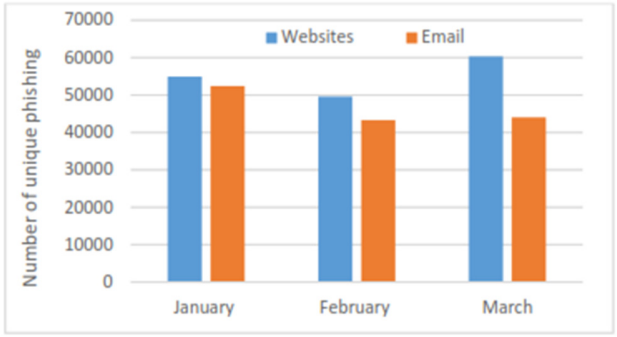

Fig. 1. Unique phishing websites and emails in Q1 of 2020.

In addition to the usual fake websites and phishing emails, cybercriminals rely on social engineering techniques to exploit human psychology to deceive people. The prevalent human weaknesses cybercriminals exploit include the inability of the people to differentiate real enterprise websites from spoofed ones, the way people interact with systems, the way people understand various alert messages and clues, and so forth. In addition, the attackers frequently use factors such as urgency or intimidations to compel the potential victims. The unsuspecting users are lured to click on a malicious link embedded in emails, which may activate a trustworthy looking spoofed website to disclose sensitive personal or financial information. Cybercriminals use sensitive information illegally harvested from victims for illicit purposes that include identity theft, financial fraud, and corporate espionage [2].

II. PHISHING THREAT LANDSCAPE

With the advances in technical countermeasures making penetration of corporate networks quite difficult, cybercriminals are shifting their focus to exploiting the easier human vulnerability to perpetrate an attack. This shift has made phishing threats prevalent and costly. According to the Anti-Phishing Working Group (APWG), phishing attacks have consistently increased over the last ten years [1]. As phishing threats are gaining prominence and techniques to prevent them are developing, phishers are getting more creative by coming up with new tactics and crafting sophisticated messages to

Corresponding author: Abdulbasit Darem

evade detection by both people and the anti-phishing measures in place.

Until recently, phishing attacks were largely dependent on spoofed websites and emails. Currently, the phishers are also taking advantage of varied channels, in addition to the conventional email messages, such as social media, SMS/text phishing (smishing), Business Email Compromise (BEC), and voice phishing (vishing). Figure 2 shows the recent phishing attack distribution based on specific channels [3]. The study is based on approximately 50 million simulated phishing attacks. It showed BEC-based and social media-based phishing attacks taking prominence over other platforms [3]. For example, with a 176% perennially increase in phishing Uniform Resource Locator (URL), Facebook has become the favor platform for phishing attacks [4]. Recently, social network sites with malicious links masked as fake news are used [5]

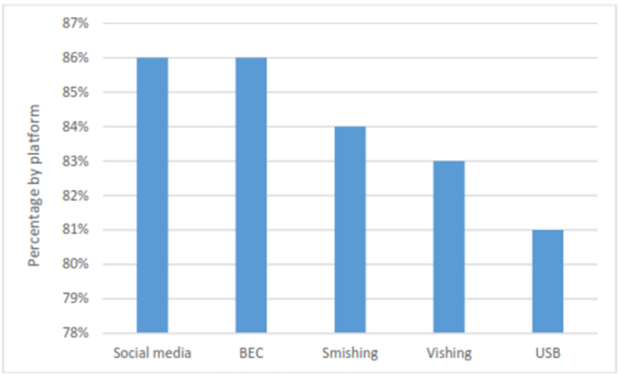

Fig. 2. Phishing attack channels.

Another channel being quietly exploited by cybercriminals is the HTTPS (Hypertext Transfer Protocol Secure) protocol. Exiting web browsers use the HTTPS protocol to alert users when they are attempting to access an "unsecure" website. An increasing practice by cybercriminals is to set up phishing sites that use the HTTPS protocol. Currently, almost 60% of phishing websites use HTTPS [1] to give a false sense of security to unsuspecting victims. Since the fake websites use HTTPS protocol, the web browsers may not flag the fake website as unsecured to the end users. This makes it very difficult for the end users to recognize it as fake. Therefore, fake HTTPS-based websites have become so prevalent that solely relying on conventional representations of Internet security is no longer trusted. Mobile-based [6] and USB-based [7] phising attacks are other channels that are increasingly exploited by cybercriminals. For example, SMS phishing that targets consumers (e.g. major bank customers) and enterprises is on the rise. With 84% of the customers reporting SMS/text phishing attacks [7], smishing volume is clearly on the rise. A study was carried out in [8] in order to see if people would take a USB flash drive left on various locations of a university campus and plug it to their computer. They found that 45% of people did plug them into their device, as well as opened a file on that USB. This problem is becoming a concern as a recent study shows that 81% of businesses in the study had suffered from malicious USB drops [7].

Cybercriminals are introducing innovative techniques to increase the success rate of phishing attacks and defeat the anti-phishing tools and the effectiveness of intervention programs. The growth of the phishing attack variety and techniques further highlights the shift of the burden of action from an automated exploit or tool to a human intelligence.

III. PHISHING THREAT CHALLENGES

The main challenge cybersecurity professionals face is finding ways to defend enterprise networks effectively and efficiently against attacks that manipulate human frailty. Addressing this challenge is very important for several reasons. In particular, with phishing attacks known to be the most frequent first step in penetrating the defenses of a firm network, the sooner a phishing attempt is detected in the attack chain, the higher the chances of stopping, containing and responding to the attack are. Normally, corporations have technical defenses in place to detect and stop phishing messages before they reach the inboxes of the employees. However, cybercriminals are innovating new tactics and are refining their attack techniques. As a result, phishing attacks are becoming more sophisticated and evading detection even by advanced technical countermeasures [9-11]. The literature discusses several possible ways to identify phishing attempts based on various clues that are visible with the naked eye. These clues include the absence of HTTPS in browsers URL, the content of web browsers, the warning signs displayed by browser toolbars, the various signs for valid certificates (e.g. VeriSign certificates), and the content and the context of the email message. Unfortunately, many people are unaware of security warnings and clues that are displayed on web browsers, or simply disregard them [12]. In addition, it is not easy for average online users to recognize phishing signs or visually identify a spoofed website [13]. Phishing attacks can be identified just by looking at the Uniform Resource Locator (URLs), even though recognizing an impersonated URL from a real one just by looking is not easy [14].

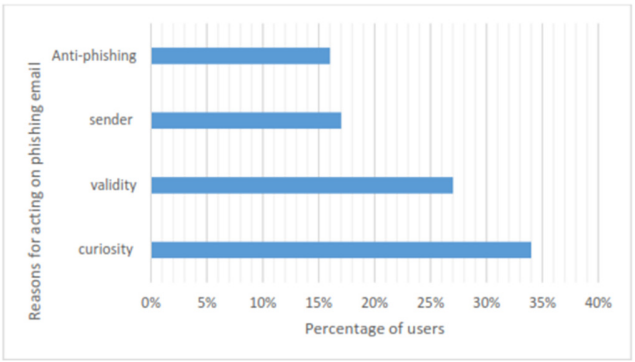

Fig. 3. Reasons for acting on phishing emails.

There are various reasons for the reaction of people to phishing messages, which make dealing with phishing threats very challenging. For example, curiosity, anti-phishing countermeasures, knowledge of the sender, and interest in validating the message are some of the reasons that compel users to act on phishing emails [15] (Figure 3). Authors in [15]

found that 34% of the participants opened emails because they were curious about the content of the message followed by 27% by the urge to find out the validity of the email message. The appearance of a name known to the receiver in the email body impersonating as the sender (even though the sender addresses are different) as well as the trust on the existence of technical anti-phishing measures are some of the reasons that make users to act on phishing emails.

To summarize, with cybercriminals resorting to more sophisticated phishing techniques, strategies, and different channels, phishing is becoming a harder and harder problem to solve. Therefore, the main objective is to minimize the success of phishing and the consequences through complementary means to advanced technical countermeasures. Specifically, phishing threats cannot be controlled by technical controls alone, thus it is imperative for businesses to complement their cybersecurity with awareness programs that successfully fight against phishing attacks.

IV. DELIVERY METHODS' COMPARISON

In this section, we analyze the various delivery methods along with various factors as shown in Table I. Regarding face-to-face delivery methods such as lectures and workshop-based methods, the training time, place, and topic of training are well known in advance. In the self-based class of delivery methods, such as the web-based, the time and place are decided by the trainee while the topic of the training may be known in advance.

Lecture and workshop-based delivery methods are generally moderated by an expert with different levels of involvement. The training is conducted onsite (e.g. classroom) thus the learners and the instructors are required to be physically present in the classroom. All other delivery methods are conducted in a virtual classroom without the physical presence of the instructors and learners. Normally the content in the self-directed delivery methods tends to be generic often developed with a one-size-fits-all scenario. On the other hand, the content in lecture-based training can be adjusted by the instructors to cater to the requirements of the learners. The instructors can also adapt lesson plans to the specific requirements of the learners. The main difference between the story-based method and the other methods, is that the content of the lesson is always written from the perspective of real experiences on an individual, whereas in the other methods, it is written from the perspective of experts. Embedded training is an ongoing real-time training and thus does not require allocation of training timetable [16-17]. As the lecture and workshop-based training methods are highly customizable, it is possible to tailor them to meet the needs of a workforce in a specific division. The trainers in the lecture-based and workshop-based training have an active presence while the instructor is passive in self-directed approaches. A marked difference between the lecture-based and workshop-based methods is the way the knowledge is transferred. In the lecture-based method, the transfer is from the instructor to the trainees, while, in workshop-based training, the knowledge is generated and shared by the participants with occasional contribution from the instructors. Also, the instructor in the lecture-based training has an active involvement in the delivery of the training content, whereas the involvement of the instructor in the workshop-based training is restricted almost to an observer level. Because employees have to be away from their regular work for the duration of the training, lecture-based and workshop-based trainings tend to be held infrequently. Additionally, both may require more time to complete than the other delivery methods. In the lecture-based training, the communication between the instructor and the learners is one-way. In contrast, the communication in the workshop-based delivery method is many-to-many because the method is based rather on dialogue than on instructions. Communication in all other methods is one-to-one, meaning there is no direct instructor involvement but the communication with the content prepared by the lectures. The problem with the later delivery methods is that if the learners want to apply what they have learnt to specific examples, they must do so on their own. Another obvious drawback is the absence of interaction with other learners and instructors, which means that learners must research and find out on their own what is not clear to them. With the provision to start studying at a time of their choice and proceed at their own pace, learners in self-directed methods must be able to self-motivate in order to finish the lesson.

As learners advance through their training program, it is necessary to track a range of metrics (e.g. participation rate, course completion rate), monitor progress, and reporting. All delivery methods except story-based and embedded-based are capable of tracking the participation rate and the completion rate. Note that in the story-based and embedded-based, an intervention for the end-users who fail the simulated phishing test is prescribed. There is no mechanism to ensure that the end users successfully complete the recommended intervention. But the end-users may or may not follow the recommendations. Only the web-based training method and the video-based and game-based delivery methods have real time reporting to answer queries regarding how many employees have completed the lesson and how many are in the progress.

The lessons in the lecture-based and workshop-based delivery methods have a fixed time to start and end, and thus they are not self-paced. The lecture-based training runs approximately 45 minutes in a classroom. For example, it run for 45 minutes in [18] and for 30 to 45 min in [13]. Since the lecture-based and workshop-based delivery methods are generally moderated by an expert, the pace is determined by the lecturer. In the story-based and the embedded-based delivery methods, the training must be done immediately after the instantiation of the lesson, and thus there is no specific time limit. The self-directed delivery methods allow the learners to choose the pace, sequence, and content of their training material. Video-based learning is flexible, and users could watch and rewatch the videos as they wish [31]. This is generally true for game-based learning. Some game-based learning progresses are controlled in such a way that the learner must achieve certain threshold in terms of correctly identifying phishing and genuine URLs [18].

Feedback is a core component in providing an effective learning experience to learners. The lecture-based delivery method, due to the active presence of the instructor during the training, offers real-time feedback [19]. The workshop-based

and the game-based [20] delivery methods also offer real-time feedback for the same reason. The embedded delivery method provides quick and useful feedback to the end users at the very moment when they make mistakes [21]. The story-based delivery method that implements the embedded training [22] also provides instant feedback. However, text-based delivery does not offer feedback or other interactive elements due to the static nature of the content format. Video-based delivery also does not provide feedback.

V. ANALYSIS OF THE DELIVERY MODELS

The current research suggests that different training delivery methods have different outcomes on the learners' ability to recognize and mitigate phishing threats [18, 21]. With this in mind, we reviewed some of the user studies with a focus on those that consider two or more delivery methods. This will shed some light on the delivery methods that are most effective in enabling learners to identify and mitigate phishing threats. Table I summarizes the various research results we considered.

TABLE I. COMPARATIVE ANALYSIS OF THE DELIVERY METHODS

Delivery Method									Satisfaction				Communication tracking				
Reference	Lecture	Workshop	Story	Text	Web	Video	Game	Embedded	Preference	Click rate	False negative	False positive	Self-efficacy	Many-many	Participate	Completed	Reporting
[27]	×	√	√	×	×	√	√	×	√	×	×		√	√	√	√	×
[2]	×	×	×	√	×	√	√	×	√		×	×	×	×	×	×	×
[16]	×	×	×	√	√	√	√	√	√	×	√	√	×	×	√	√	×
[28]	√	×	×	√	×	√	√	×	×	√	×		√	√	×	×	√
[29]	×	×	×	×	√	×	√	×	×	√	×		√	√	×	×	√
[30]	√	×	×	√	×	×	√	×	×	√	×		√	√	×	×	√
[31]	×	×	√	×	√	×	×	×	×	√	×		√	√	×	×	×
[32]	×	×	√	×	√	×	×	×	×	√	×		√	√	×	×	×

Authors in [23] tested the efficacy of embedded phishing with a web-based training page to see if it improves the phishing awareness of the users. The study considered 1,359 corporate employees. The authors organized the outcome of the evaluation in terms of click rate as: people who always clicked (Always) irrespective of previous training about phishing, people who clicked at least once (Once), people who clicked after training (Trained), and people who never clicked (Never). The result showed that anti-phishing education works as demonstrated by nearly 63% reduction of the click rate after the training. This study revealed that there are people who ignore security training and advice. The main reasons for the end user's decision to accept or ignore security advices are investigated in [24-25]. The authors revealed that perceived trust of the security advice sources as the main reason for accepting it while factors such as inconvenience, privacy concerns, and excessive information are grounds for rejecting the security advice. Authors in [26] determined that fear of consequences of clicking or not clicking as the main driver for people to act on phishing emails. A summary of the results of the works of Wash and Cooper [31], Marsden et al. [32] and Caputo et al. [23] in terms of click rate by the study subjects is shown in Figure 5. The results of these studies show that there is a correlation between the performance of the training and the different class of subjects. Therefore, it is paramount to consider the demographic information of the subjects when designing and delivering intervention training.

Several user studies that measure the efficacy of game-based training method as compared to other delivery methods exist. Authors in [29] evaluated the effectiveness of game-based delivery method in raising phishing attack awareness. They compare it to a web- based delivery method (i.e. tutorial information given in APWG website on phishing). In terms of recognizing fake websites, the result showed that the end-users trained with game-based delivery method were able to recognize a fake site with a higher rate of accuracy than the participants who were trained using a website.

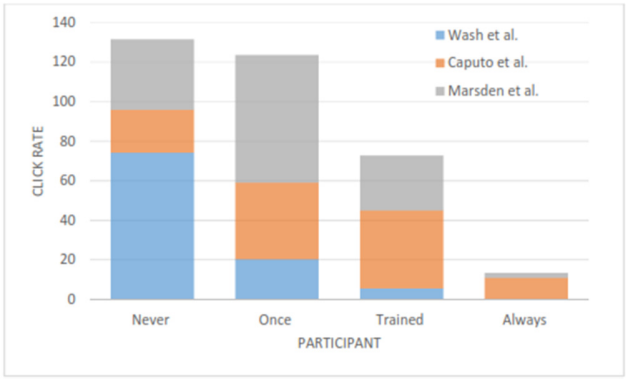

Fig. 4. Participants click rate characteristics.

Authors in [16] evaluated the efficacy of embedded training to improve end user susceptibility to phishing threats using the False Positive (FP) and False Negative (FN) metrics. A FP happens if a user identifies a genuine website as a phishing one while a FN occurs if a user wrongly identifies a phishing website as a genuine website. Different training delivery methods, namely game-based, web-based/video-based, and text-based were considered. The participants received several simulated phishing emails. A remedial training is randomly offered from the list of the four embedded training methods to the end users who clicked on the embedded link in the simulated emails. After the training, another set of simulated phishing emails were sent to the same end users and then it was behaviorally measured whether they fell victims to

the phishing attacks or not. The outcome of the study is summarized in Table II. The overall result shows that the end users correctly recognize phishing links in a significantly better rate after the training. Participants trained with game-based delivery method performed better overall. This may be due to the fact that they performed the post-training test immediately after training. The result also shows that training with game-based methods is as good as the web-based in regard to FN but better in terms of FP. Although the game-based delivery method is able to decrease FP from an original 30% to 14%, as well as FN from the original 34% to 17%. Unfortunately, the result shows that a significant number of end users are still susceptible to phishing threats.

TABLE II. EMBEDDED TRAINING PERFORMANCE ANALYSIS

Evaluation	Text-based		Game-based		Web-based	
	FP	FN	FP	FN	FP	FN
Pre-training	27%	43%	30%	34%	30%	38%
Post training	21%	19%	14%	17%	41%	12%

Authors in [27] conducted a user study of game-based delivery method and compared it against web-based [33] using 39 students at Cornell. The game used in study was What.Hack [27] and the web-based training material [33]. The participants were given a pretest, training, and a posttest, in that sequence. The effectiveness was measured using the correctness percentage (click rate). The result of the experiment shows a significant improvement for game-based delivery method from 65% before training to 89% after training (about 37% improvement) in correctly recognizing phishing attempts. The performance of the web-based delivery methods of Wash et al. [31] and Wen et al. [27] is compared in Figure 5.

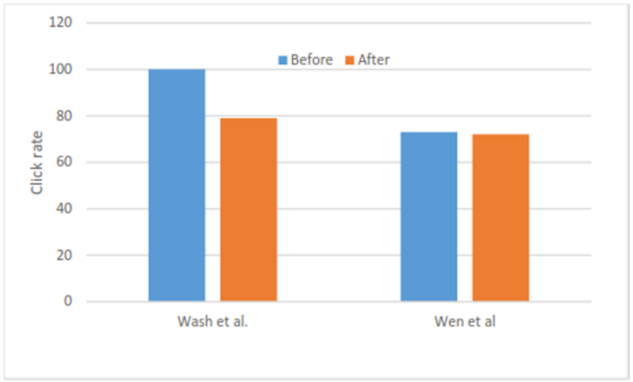

Fig. 5. Web-based delivery method outcome.

The result shows that training reduces the susceptibility to phishing threats but incorporating lecture-based training does not have significant changes. Following training, both groups substantially reduced the threat. The authors also considered the confidence level of the participants after training. The learners' self-confidence based on self-assessment showed that the learners showed strong confidence in their ability to recognize phishing emails. The result also suggested that preference for lecture-based delivery method is higher than the other methods.

TABLE III. COMBINED TRAINING PERFORMANCE ANALYSIS

Evaluation	Group A		Group B	
	Click rate	Data divulge	Click rate	Data divulged
Pre-training	13.2% (9/68)	77.77% (7/9)	3.1% (2/56)	50% (1/2)
Post training	1.5% (1/68)	100% (1/1)	1.6% (1/56)	100% (1/1)
Reduction	11.4%		51.6%	

VI. CONCLUSION

This paper provides a review of the delivery methods of cybersecurity training programs aimed at improving personnel's awareness and behavior of information security in the context of phishing. The phishing landscape and challenges were addressed. The delivery methods were analyzed to shed some light on the delivery that is most effective in enabling learners to identify and mitigate phishing threats. The delivery methods along with their various factors were analyzed. In face-to-face delivery methods, such as lecture and workshop-based methods, training time, place, and topic of training are well known in advance. In the self-based class of delivery methods such as the web-based, the time and place are decided by the trainee while the topic of the training may be known in advance. The web-based delivery method performance for several studies was compared to observe that after training, the click rate decreases by 21% which suggests that training does decrease susceptibility to phishing threat to certain extend. The result also suggested that the preference for the lecture-based delivery method is higher than for the other methods.

REFERENCES

[1] APWG, *Phishing Activity Trends Report*, 1st Quarter. Anti-Phishing Working Group, 2020.

[2] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behaviour & Information Technology*, vol. 33, no. 3, pp. 237–248, Mar. 2014, https://doi.org/10.1080/0144929X.2012.708787.

[3] "2021 Report on Phishing Attacks - State of the Phish," *Proofpoint*, Mar. 30, 2021. https://www.proofpoint.com/us/resources/threat-reports/state-of-phish (accessed Nov. 23, 2021).

[4] "Facebook Phishing: Why Social Media is a New Phishers' Favorite," *Vade Secure*. https://www.vadesecure.com/en/blog/facebook-phishing-is-exploding (accessed Nov. 23, 2021).

[5] E. D. Frauenstein and S. Flowerday, "Susceptibility to phishing on social network sites: A personality information processing model," *Computers & Security*, vol. 94, Jul. 2020, Art. no. 101862, https://doi.org/10.1016/j.cose.2020.101862.

[6] D. Goel and A. K. Jain, "Mobile phishing attacks and defence mechanisms: State of art and open research challenges," *Computers & Security*, vol. 73, pp. 519–544, Mar. 2018, https://doi.org/10.1016/j.cose.2017.12.006.

[7] *2021 Report on Phishing Attacks - State of the Phish*. Proofpoint, 2021.

[8] M. Tischer *et al.*, "Users Really Do Plug in USB Drives They Find," in *IEEE Symposium on Security and Privacy*, San Jose, CA, USA, May 2016, pp. 306–319, https://doi.org/10.1109/SP.2016.26.

[9] S. Nasiri, M. T. Sharabian, and M. Aajami, "Using Combined One-Time Password for Prevention of Phishing Attacks," *Engineering, Technology & Applied Science Research*, vol. 7, no. 6, pp. 2328–2333, Dec. 2017, https://doi.org/10.48084/etasr.1510.

[10] A. Al-Marghilani, "Comprehensive Analysis of IoT Malware Evasion Techniques," *Engineering, Technology & Applied Science Research*, vol. 11, no. 4, pp. 7495–7500, Aug. 2021, https://doi.org/10.48084/etasr.4296.

[11] D. K. Singh and M. Shrivastava, "Evolutionary Algorithm-based Feature Selection for an Intrusion Detection System," *Engineering, Technology & Applied Science Research*, vol. 11, no. 3, pp. 7130–7134, Jun. 2021, https://doi.org/10.48084/etasr.4149.

[12] M. Alsharnouby, F. Alaca, and S. Chiasson, "Why phishing still works: User strategies for combating phishing attacks," *International Journal of Human-Computer Studies*, vol. 82, pp. 69–82, Oct. 2015, https://doi.org/10.1016/j.ijhcs.2015.05.005.

[13] R. M. Mohammad, F. Thabtah, and L. McCluskey, "Tutorial and critical analysis of phishing websites methods," *Computer Science Review*, vol. 17, pp. 1–24, Aug. 2015, https://doi.org/10.1016/j.cosrev.2015.04.001.

[14] J. S. Tharani and N. A. G. Arachchilage, "Understanding phishers' strategies of mimicking uniform resource locators to leverage phishing attacks: A machine learning approach," *Security and Privacy*, vol. 3, no. 5, 2020, Art. no. e120, https://doi.org/10.1002/spy2.120.

[15] Z. Benenson, "Exploiting curiosity and context: How to make people click on a dangerous link despite their security awareness," presented at the Black Hat USA 2016, 2016.

[16] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching Johnny not to fall for phish," *ACM Transactions on Internet Technology*, vol. 10, no. 2, pp. 7:1-7:31, Jun. 2010, https://doi.org/10.1145/1754393.1754396.

[17] J. Hong, "The state of phishing attacks," *Communications of the ACM*, vol. 55, no. 1, pp. 74–81, Jan. 2012, https://doi.org/10.1145/2063176.2063197.

[18] K. RaniSahu and J. Dubey, "A Survey on Phishing Attacks," *International Journal of Computer Applications*, vol. 88, pp. 42–45, Feb. 2014, https://doi.org/10.5120/15392-4007.

[19] P. Kim, J. V. Homan, and R. L. Metzer, "How long do employees remember information security training programs? A study of knowledge acquisition and retention," *Issues in Information Systems*, vol. 17, no. 4, pp. 197–207, 2016.

[20] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: state of the art and future challenges," *Neural Computing and Applications*, vol. 28, no. 12, pp. 3629–3654, Dec. 2017, https://doi.org/10.1007/s00521-016-2275-y.

[21] "The Art of Deception in Social Media Phishing." https://www.vadesecure.com/en/blog/the-art-of-deception-in-social-media-phishing (accessed Nov. 23, 2021).

[22] I. Qabajeh, F. Thabtah, and F. Chiclana, "A recent review of conventional vs. automated cybersecurity anti-phishing techniques," *Computer Science Review*, vol. 29, pp. 44–55, Aug. 2018, https://doi.org/10.1016/j.cosrev.2018.05.003.

[23] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, and M. E. Johnson, "Going Spear Phishing: Exploring Embedded Training and Awareness," *IEEE Security Privacy*, vol. 12, no. 1, pp. 28–38, Jan. 2014, https://doi.org/10.1109/MSP.2013.106.

[24] E. M. Redmiles, S. Kross, and M. L. Mazurek, "How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior," in *ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, Oct. 2016, pp. 666–677, https://doi.org/10.1145/2976749.2978307.

[25] E. M. Redmiles, A. R. Malone, and M. L. Mazurek, "I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security," in *IEEE Symposium on Security and Privacy*, San Jose, CA, USA, May 2016, pp. 272–288, https://doi.org/10.1109/SP.2016.24.

[26] K. Greene, M. Steves, and M. Theofanos, "No Phishing beyond This Point," *Computer*, vol. 51, no. 6, pp. 86–89, Jun. 2018, https://doi.org/10.1109/MC.2018.2701632.

[27] Z. A. Wen, Z. Lin, R. Chen, and E. Andersen, "What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game," in *CHI Conference on Human Factors in Computing Systems*, Scotland, UK, May 2019, pp. 1–12, https://doi.org/10.1145/3290605.3300338.

[28] K. F. Tschakert and S. Ngamsuriyaroj, "Effectiveness of and user preferences for security awareness training methodologies," *Heliyon*, vol. 5, no. 6, Jun. 2019, Art. no. e02010, https://doi.org/10.1016/j.heliyon.2019.e02010.

[29] N. A. G. Arachchilage, S. Love, and K. Beznosov, "Phishing threat avoidance behaviour: An empirical investigation," *Computers in Human Behavior*, vol. 60, pp. 185–197, Jul. 2016, https://doi.org/10.1016/j.chb.2016.02.065.

[30] S. Stockhardt *et al.*, "Teaching Phishing-Security: Which Way is Best?," in *International Conference on ICT Systems Security and Privacy Protection*, Ghent, Belgium, Jun. 2016, pp. 135–149.

[31] R. Wash and M. M. Cooper, "Who Provides Phishing Training? Facts, Stories, and People Like Me," in *CHI Conference on Human Factors in Computing Systems*, Montreal, QC, Canada, Apr. 2018, pp. 1–12, https://doi.org/10.1145/3173574.3174066.

[32] J. Marsden *et al.*, "Facts and Stories in Phishing Training: A Replication and Extension," in *Conference on Human Factors in Computing Systems*, New York, NY, USA, Apr. 2020, pp. 1–6, https://doi.org/10.1145/3334480.3381435.

[33] Barracuda Networks Inc, "Click Thinking Content," *Barracuda Campus*. https://campus.barracuda.com/product/phishline/doc/79463828/click-thinking-content/ (accessed Nov. 23, 2021).