Taxonomy of Cybersecurity Awareness Delivery Methods: A Countermeasure for Phishing Threats

Asma A. Alhashmi[1], Abdulbasit Darem[2], Jemal H. Abawajy[3]
Department of Computer Science, Northern Border University, Arar 91431, Saudi Arabia[1, 2]
Cybersecurity Research and Innovation Centre, Deakin University, Burwood, VIC 3217, Australia[3]

***Abstract*—Phishing is a serious threat to the Internet users and has become a vehicle for cybercriminals to perpetrate large-scale crimes worldwide. A wide range of technical and educational measures have been developed and used to address phishing threats. However, the technical anti-phishing measures have been widely studied in the current literature whereas comprehensive analysis of the non-technical anti-phishing techniques has generally been ignored. To close this gap, we develop a new taxonomy of the most common cybersecurity training delivery methods and compare them along various factors. The work reported in this paper is useful for various stakeholders. For organizations conducting or considering phishing training, it helps them understand the various awareness training and phishing campaigns capabilities and design an appropriate program with a meaningful return. For researchers, it offers a clearer understanding of the main challenges, the existing solution space, and the potential scope of future research to be addressed.**

***Keywords*—Phishing attack; human factors in cybersecurity; cybersecurity threats; cybersecurity awareness; anti-phishing awareness delivery methods**

I. Introduction

Internet technology coupled with advances in mobile devices such as smartphones have enabled regular every-day people to learn, work, purchase, entertain, connect, and network from anywhere and at any time. With the increasing reliance on the Internet, so is the threat of being falling a victim to cybersecurity attacks. Cybercrime is the fastest growing crime worldwide and continue to increase in sophistication and costs to the global economy with an estimated $6 trillion by 2021 [4]. Phishing is the most prominent attack vector used by cyber criminals today and phishing prevalence is at all-time high [5]. Phishing impacts online users and organisations of all size and sectors including banks and public services. The financial costs to victims due to phishing attacks worldwide are staggering and currently estimated to surpass a trillion dollars [38]. In the U.S. alone, the financial costs to businesses between 2013 and 2019 are estimated to be more than $10 billion [17]. With phishing attacks accounting close to 90% of the estimated cybercrime costs [10], there is a substantial economic benefit for putting in place appropriate anti-phishing measures to fight phishing threats. As a result, a serious effort to combat phishing threats has been pursued both in academia and industry.

Various technical measures have been proposed in the literature to address phishing threats. These automated anti-phasing measures include email filtering [1,7], machine learning based techniques to identify phishing emails and websites [20], and browser security indicators that warn end-users potential dangers from malicious email messages and fake websites [23]. Although automated anti-phishing solutions are powerful defence, phishing attacks remain a significant threat to individuals and businesses currently accounting for more than 80% of reported security incidents [24]. Moreover, it takes 32 days on average for technical countermeasures to detect and mitigate phishing attacks [42]. In addition, cybercriminals continue to become more creative and changing tactics to get around the anti-phishing measures in place and sending much more plausible-looking phishing messages [39]. Therefore, despite considerable advances in anti-phishing technical solutions, the automated anti-phishing measures are still inadequate to combat phishing threats [33].

Cybercriminals are increasingly shifting from exploiting software and hardware vulnerabilities to depending on human weaknesses to perpetrate an attack on individuals and businesses. For phishing threats to be realised, the cyber attackers must first institute a trust with the potential victims. This means automated solutions alone do not provide complete safeguard against phishing attacks. Since phishing attacks primarily exploit human vulnerability, human intelligence based anti-phishing approach is the best defence to narrow the gap left by technical measures. Therefore, intervention programs that improve human awareness and security behaviour have been developed to augment the technical solutions. These intervention programs implement different delivery methods to build vital security awareness skills and changes both awareness and behaviour of the end users.

This paper provides a new taxonomy of the most common cybersecurity training delivery methods developed to train the workforce to protect themselves from phishing threats. Second, we will survey and critically analyse a variety of phishing awareness delivery methods based on the taxonomy we developed with emphases on those that focus on what delivery methods are effective in increasing the ability of the people to detect and mitigate phishing threats. This provides useful information that will enable organisations to explore various alternatives when conducting workforce security awareness training. Third, existing literature does not provide basses for future researchers to build on in the cybersecurity awareness training sphere [14]. There are state-of-the-art reviews on various aspects of the technical solutions for phishing attack [1,3,6,8,12,19,27-28,36,43]. However, there is no work to the best of our knowledge that has conducted a review of the

Grant no. SAT-2018-3-9-F-7926 from the Deanship of Scientific Research at Northern Border University, Arar, K.S.A.).

literature about cybersecurity awareness training methods. Therefore, this study is useful for future researchers interested in developing human intelligence based anti-phishing countermeasures to combat phishing threats.

This paper is structured as follows: Section 2 presents phishing awareness techniques and the taxonomy of the delivery methods. Comparison of the delivery methods along various factors is also presented. Section 4 presents some open problems for future research. Section 5 discusses the conclusions.

II. Anti-Phishing Cybersecurity Intervention Programs

Cybercriminals are increasingly targeting employees across all sectors to infiltrate corporate networks to steal confidential client data and corporate secrets. Phishing attempts that normally evaded detection by the technical measures put in place are often recognized and reported by employees [11]. Therefore, fortifying end users to defend themselves against phishing threats through cybersecurity intervention program such as phishing awareness training is necessary to thwart phishing attacks.

A. Cybersecurity Awareness Training

For organisations to ensure that their employees contribute to the enterprise cybersecurity program, employees should be provided with regular cybersecurity training so that they are able to make appropriate choices to prevent or mitigate the risks posed by phishing attacks. The primary aim of the anti-phishing intervention program is to improve cybersecurity awareness and behaviour at workplace by reducing end-user susceptibility to phishing threats.

Therefore, we define cybersecurity awareness training as

'a proactive measure deployed to combat cybersecurity threats using various delivery methods to raise end-user's awareness and foster secure behaviour with overall aims of empowering users to recognise and report malicious activities in a timely manner and use best cybersecurity practices in daily routine.'

Anti-phishing cybersecurity intervention program empowers end users and employees to recognize and neutralize phishing cyberattacks. In order for the enterprise cybersecurity intervention program to yield positive awareness and behaviour, employees should be given cybersecurity training intervention on the threats posed by phishing attacks, how to identify phishing attempts such as malicious websites, and how to take the appropriate decisions to prevent or mitigate phishing attacks [16]. Such anti-phishing intervention program will pay dividends to the organisation by protecting businesses from adverse disastrous consequences, which includes data breaches, business continuity issues (e.g., due to ransomware attacks), reputational damages, financial loses and much more. This is confirmed by a recent large-scale study that included various parts of the world (i.e., the UK, France, Germany, Spain, the US, Australia, and Japan) found that about 78% of firms involved in the study indicated that their cybersecurity awareness training resulted in measurable declines in phishing attack vulnerability [35].

There is a general consensus within the existing literature that cybersecurity intervention program can minimize human factors related cybersecurity issues including phishing threats [2,3,8,9,13,15,26,41]. For example, the study by Sheng et al. [41] showed that cybersecurity intervention programs are effective and decreased by 40% the people who enter confidential and sensitive information on fake webpages. Therefore, cybersecurity awareness and training of employees become extremely crucial in keeping enterprises and organizations better protected from phishing attacks. There are a wide range of cybersecurity awareness training intervention programs that train, educate, and persuade end users against phishing attacks. The intervention programs to instil vital security awareness skills and subsequently bring changes in employee cyber behaviours are implemented using different delivery methods. Therefore, for the cybersecurity intervention program to be effective and successful in reducing human factor related security issues, appropriate delivery methods for cybersecurity awareness training intervention programs should be used. In the next section, we propose a new taxonomy of the delivery methods.

B. Taxonomy of Delivery Methods

Cybersecurity awareness program to raise awareness and educate users on phishing attacks is conducted using one or more delivery methods. There are various types of cybersecurity training and awareness delivery methods. In this section, we discuss the most prominent delivery methods.

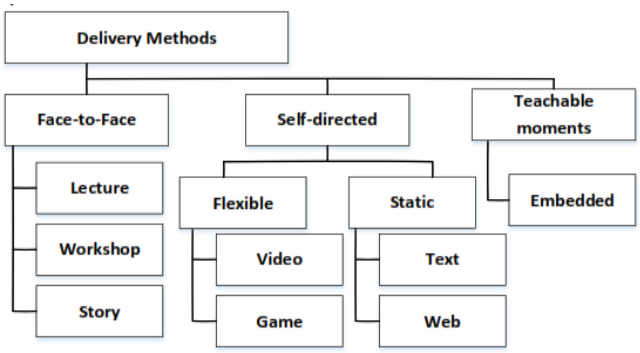

Fig. 1. Taxonomy of Cybersecurity Training Delivery Methods.

Fig. 1 shows the proposed taxonomy of cybersecurity awareness training delivery methods. Basically, we classify the delivery methods into three main classes namely, face-to-face class, self-directed class, and embedded class. The self-directed class of the delivery method is further sub-divided as flexible and static categories. In the following subsections, we describe each in detail.

1) Face-to-face delivery methods: The face-to-face cybersecurity intervention program delivery method involves physical learning environment with or without direct involvement of cybersecurity expert as a facilitator. Examples of such delivery methods are a lecture-based, a workshop-based and a story-based delivery method.

a) Lecture-based delivery method: Lecture-based cybersecurity intervention program delivery method is one of the most prevalent delivery methods [22,26,42]. The training

primarily consists of formal presentations (i.e., lectures) by an instructor in a classroom setting for a group of participants. The instructor may use power point slides as well as other resources such as audio-visual aids. The lecture is delivered by a security expert (instructor) and requires physical attendance of both the learners and the instructor in the classroom.

Although the knowledge transfer is one way (i.e., form the expert to the learners), it encourages direct interaction between learners and the instructor. Through incorporating group learning activities, it can also enable interaction as well as collaboration among the trainees allowing the learners to learn from each other. It also has the flexibility of providing tailored session to the specific industry or a particular department within a workplace. The learners can ask for further clarifications on concepts that are not clear in the class, and any question and doubt can be addressed immediately during the session.

Lecture-based delivery method is relatively costly as it includes expenses related to hiring the instructor, preparation of the content and the employee time away from their regular jobs. A major challenge of the lecture-based method is ensuring the engagement of the participants and avoiding boredom. This challenge can be easily addressed by initiating short breaks when attendees become distracted or bored and include activities that require the participants apply the concepts covered to their role or quizzes throughout the session.

b) Workshop-based delivery method: Workshop-based cybersecurity intervention program emphasises dialogue and plenary reflection with the ideal size of about 15 participants over several plenary discussions [13]. The participants are divided into small groups of individuals. Each group is allotted a timeframe to discuss on a given cybersecurity-related scenario among themselves to create a reflection. This is followed by a plenary discussion where each group presents its possible answer to their scenario and then the other groups were asked to provide their comments on the response provided by the group. Each plenary session is closed by a brief concluding remark of the instructor on the scenario followed by questions or remarks from the workshop participants.

Workshop-based training is similar to the lecture-based training in that it involves an expert and attendees gathered in a workshop venue such as classroom. Unlike the lecture-based program where the expert drives the training, the role and involvement of the expert is restricted mainly to define the workshop topics, develop learning materials needed for the session, manage time, occasionally answering specific questions directed to the expert during the workshop, and ensuring that the workshop discussion remain within the scope of the defined topic. The workshop participants drive the training through dialogue, participation, and collective reflection in small groups [13]. The workshop attendees steer most of the discussions among themselves by actively exchanging their thoughts with each other and the instructor in plenary reflections.

c) Story-based delivery method: Story-based cyber security awareness uses narrative stories about real-life cybersecurity events to train employees about security as a relatable experience [30,39]. A personal story narrative may contain information about the approach used by the phisher to deceive the storyteller, the consequences of being phished and what steps to take not to make similar mistakes. Basically, the story-based training explores the intuition that people tend to learn about cyber security by hearing positive and/or negative real stories as well as security warnings from experts/peers.

For example, people who have personally experienced security attacks such as identity theft learn a hard way about security threats and how to better protect themselves against attacks. Wash and Cooper [39] used social stories about prior experience of phishing attacks to train employees in an organisation and tested to see if the employees can recognise and avoid falling victim to phishing attacks. They found that stories are more effective when the learners think that the stories originate from people with similar characteristics.

2) Self-directed delivery methods: The cybersecurity awareness training delivery methods within the self-directed category includes the delivery methods that cater to virtual learning environment and learners' self- regulation. It can be divided into two subcategories; one is Flexible category and the other is static category. Examples of self-directed delivery methods include we-based training, text-based, video-based, and game-based approaches.

a) Video-based delivery: In the video-based awareness delivery method, a 2-to-5-minute micro-learning style videos used are used for self-directed learning about phishing and how to defend against it. It is a self-paced learning where the learner can pause the video at any time and re-watch it later. The content normally contains real scenarios and examples in the form of clips, animation, and cartoons related to phishing attacks. For example, the phishing awareness video developed by Volkamer et al. [32] includes authentic-looking messages laced with tricks to seduce potential victims to click on a malicious link embedded in the message. The content also includes misconceptions about phishing normally found in the literature and warning messages such as the likely impacts of clicking on a malicious link.

The video used in Tschakert and Ngamsuriyaroj [26] is approximately 2 to 3 minutes and offers a basic overview of phishing, a brief description of the tactics used by phishers to deceive potential victims, the potential impacts, and the possible clues that can be used to recognise dishonest emails and URLs. The videos offer visual learning, which may shorten the time employees require to commit to the training. However, it could be expensive to develop and may be difficult to make the learners engaged in the content [32].

b) Game-based delivery: Educational game-based cybersecurity training provides a learning environment coupled with entrainment where employees (as players) learn phishing methods and how to detect them through playing the game. Learning takes place in a virtual environment involving teaching agent (virtual) and the learner (physical). Normally, story-based method in which the story is shown to the learners in a comic format is used. Game flows are structured on

progressive levels normally from basic to advanced levels such that players are required to successfully complete the content at a specific level before they are allowed to proceed further to a higher level. Each level is normally designed with several sequential activities/questions and the players may be forced to complete/answer each activity/question in the sequences program in the game before moving to the next activities/questions. Also, some games have built-in timer to restrict the player to complete a given activity/question within certain period. The side effect of a restriction on game play time is that it can make self-paced learning impossible.

The design's philosophy of exiting game-based cybersecurity delivery methods is summarized in [25]. Game-based training have emerged as a powerful security awareness and training delivery methods resulting in several systems such as Phishy [29], What Hack [44], and NoPhish [18]. Generally, this game-based training software that teaches end-users how to detect phishing URLs using cues, distinguish between fake and genuine sites using cues, and how to decide if a given site is legitimate or not using search engines. Asanka et al. [33] describe a mobile game-based delivery method that teaches people how to identify URL-related phishing threats such that the people who are trained with the game will be able to differentiate malicious websites from genuine ones. Game-based model are highly interactive and engaging medium. Also, it offers visual learning and has inherent option of self-paced, pausing the game and resuming it at any suitable time. A well-designed game-based training delivery method can potentially offer quick learning and proficiency of cybersecurity fundamentals [16].

c) Text-based delivery: Text-based training consists of an educational reading material that takes about 15–20 minutes. The reading material is prepared by an expert and distributed to the potential learners to master the content. Generally, the content covers topics such as "look for https", "type in URLs don't click on them", "phishing is your problem; don't rely on others to protect you", and "misspellings can signal fake emails". The content may also include examples and the description of the best security practices. In the basic form of text-based training, the learner is normally provided with a hardcopy of the material used in lecture-based training or text derived from corporate guidelines/warnings usually available on the organisation's website. However, a softcopy text in a form such as PDF require an electronic device with appropriate software (PDF reader). A tool called NoPhish [18] provides text-based delivery capability and commonly used in training [26,42].

Similar to web-based training method, text-based model has inherent option of self-paced, pausing and resuming at any suitable time and studying the material in any order. Although the reading material is expected to take 15–20 minutes of reading time, the trainees can spend as much time as they needed to go through it. Unfortunately, the text-based training is static and not interactive. Also, it does not have the option to provide feedback to the learners. Tschakert et al. [26] and Stockhardt et al. [42] used text-based delivery method for training learners on how to detect phishing emails and fake websites. The lessons cover topics on introduction to phishing, examples of phishing emails and websites as well as the possible impacts of a successful phishing attack, markers of dishonest emails and URL addresses.

d) Web-based training: Web-based delivery methods can be based on anti-phishing contents on websites (basic form) or advanced for, which we refer to as a computer-based training (CBT). In its basic form, web- based training method are freely available online resources that contain facts and advice about phishing threat, various ways to identify it, and what to do to avoid falling prey to phishing scams. Examples of the basic anti-phishing web-based training material include the Anti- Phishing Working Group website (APWG) [5] and Cornell's PhishLine [6] web pages on phishing. CBT version is normally commercially available and is advanced web-based training methods. It is generally interactive, developed on the principles of instructional design and have six basic elements that enable the learner to control his/her learning namely, capability to 'skip, supplement, sequence, pace, practice (for users to assess their understanding of phishing) and guidance identified' [37]. For example, Abraham et al. [40] discusses a web-based training method with topics covering counterfeit webpages and malicious links organized as hyper-links.

The web-based delivery method enables the learner to schedule the most convenient time to access the content of the awareness training modules, stop at any time and come back to it at a later point of time. The content can be organised in such a way that the trainees could select the topics to learn in any sequence. Normally, web-based method includes quizzes and tests that measure the performance of the trainees and provides direct feedback on the performance of the end users. Similarly, web-based training method allows for interactivity that optimizes the learning experience.

The consistency of the content and the simplicity of use are the virtues of web-based training method. Also, web-based training method is often deemed a cost-effective way of raising employee cybersecurity awareness. Web-based training method does not provide facility for further explanation, may encourage finishing the learning modules with nominal time or diligence, and it may be monotonous and unchallenging [21]. Some of these shortcomings can be addressed by incorporating resources such as visuals and animations into the content. Each learner completes the training modules online individually using desktop computers or hand-held devices (e.g., tablets, iPad, and smartphones).

3) Teachable moment delivery methods: This class of awareness delivery methods follows the test-train concept such that only people who fail the test will be trained using other delivery methods such as story-based or text-based methods. An example of this class is the embedded method discussed below.

a) Embedded delivery method: The idea of embedded phishing training is to send simulated phishing emails to users, usually without letting them know about it, to test their ability to identify phishing attempt. A user who falls for the simulated phishing attack receives a remedial training about phishing and how to recognize phishing emails immediately (known as

"teachable moments") following the click on the link. For example, an email with embedded link to an external website is sent to the employees and urged them to click on the link where they would input their login credentials. If an employee acts upon the request and clicks the link in the email, then a remedial training is provided to the employee typically a webpage where training materials are hosted. Following the remedial training, another simulated phishing emails can be used to check if the ability to detect phishing threats have improved or not.

Essentially, embedded training provides continual real time training experience to the employees by embedding the training into the day-to-day tasks the employees perform [39]. There are many tools such as PhishGuru [34] that provides an embedded training to end-users based on simulated phishing email. It is believed that embedded training can help the learners to retain the learnt knowledge for an extended period as compared to the other methods [34]. However, it can also increase the frequency of the click rate on phishing link by the end users [31].

In Table I, we show a comparative analysis of the delivery methods presented in the previous sections.

TABLE I. COMPARATIVE ANALYSIS OF THE DELIVERY METHODS

	Classroom		Pace		Feedback			Learning			Instructor		Communication			Tracking			Time
	Physical	Virtual	Lecturer	Self	None	Real	Direct	Active	collaborate	Personal	Active	Passive	One-one	One-many	Many-many	Participate	completed	reporting	Minutes
Lecture		×		×	×			×		×		×	×		×			×	30 to 45
Workshop		×		×	×			×		×		×	×					×	30 to 45
Story	×		×	×	×		×		×		×	×		×	×	×	×	×	15 to 20
Text	×		×			×	×		×		×			×	×			×	15 to 20
Web	×		×		×		×		×		×			×	×				15 to 20
Video	×		×			×	×		×		×			×	×				2 to 5
Game	×		×		×		×		×		×			×	×				30
Embedded	×		×	×	×		×		×		×			×	×	×	×	×	15 to 20

III. OPEN PROBLEMS

There has been ample research in countering phishing threats with emphases on human factor dimension with encouraging results. However, phishing threat prevalence continues and expected to remain significant problem in cybersecurity. In this section, we highlight some of the gaps that need to be closed in the current state-of-the-art phishing studies.

There are still many open problems that need to be researched. Firs, exiting research shows that the approaches proposed so far can reduce significantly click rates down to rates closer to 20% [34,39]. However, this still exposes a substantial number of users susceptible to phishing threats. Therefore, there is still room to improve exiting approaches or develop novel approaches to counter phishing attacks. Also, there is very little work in terms of retaining the acquired knowledge. This requires longitudinal study of various delivery methods.

Another area that needs to be explored is the performance of various delivery methods in a multinational environment. This requires investigating how cultural traits manifest themselves in making users susceptible to phishing attacks. There is a gap in clearly identifying what factors are responsible for exactly triggers and when a person is at most vulnerable to phishing attacks. Today, users tend to have multiple emails (e.g., work emails and outside emails such as Gmail). Some employees forward all their emails to an outside account. How this practice exacerbates the phishing attack needs to be addressed.

The attackers use a variety of persuasive techniques and channels (e.g., email, USB, social networks) to bait users into clicking on malicious links embedded in the emails or obtaining personal information. This raises several research questions. First, how effective the different persuasive techniques are in terms of enticing end users to fall prey for the phishing attacks. This research is necessary for developing an effective anti-phishing solution informed by an in-depth knowledge on the subject of persuasion techniques used by the cybercriminals. Second, how does persuasive techniques and different channels interact with user demographics to facilitate of demographically different people susceptible to phishing attack. Third, one can also consider the effect of the phishing emails content over channels and different persuasive techniques.

Several large-scale users studied in the field is really needed to validate the efficacy of the various delivery methods. Furthermore, game-based cybersecurity training for enterprise-wide users received relatively less attention in the research community. Similarly, studies with respect to the various evasive techniques employed by the cybercriminals and their degree of difficult for the end users to detect phishing threats is another research gap that need to be addressed. The challenges in how to measure the retention rate and motivate behaviour

change needs to be researched. The verdict on whether or not cybersecurity awareness training changes the behaviour of the end users has not resolved yet; finally, how to evidence the need for investment in cybersecurity awareness training.

IV. Conclusion

Phishing attacks are becoming prevalent and affecting individuals and businesses in all sectors regardless of their sizes causing losses of sensitive data and financial costs. Since phishing are only effective if they are acted upon by the end users, in addition to ensuring that technical countermeasures such as email filters are configured to prevent phishing messages from getting into employee's inbox, equipping employees with the skills necessary to protect themselves and their organization against phishing threats is a key part of a robust cybersecurity program. This paper provides a review of cybersecurity training program delivery methods used by organizations aimed at improving personnel information security awareness and behaviour in the context of phishing training. The paper also presents a description and taxonomy of the most common cybersecurity training delivery methods. Although the exiting research shows that well-crafted end-user cybersecurity awareness and training program can be very effective in minimizing susceptibility to phishing attacks, there are still room for improvement. Moreover, phishing threat remains prevalent and will continue to be a significant problem, thus more research is needed to minimize its impact.

Acknowledgment

The authors gratefully acknowledge the approval and the support of this research study by grant no. SAT-2018-3-9-F-7926 from the Deanship of Scientific Research at Northern Border University, Arar, K.S.A.

References

[1] A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg, and E. Almomani, "A survey of phishing email filtering techniques," IEEE Commun. Surv. Tutor., vol. 15, no. 4, pp. 2070–2090, 2013.

[2] A. Carella, M. Kotsoev, and T. M. Truta, "Impact of security awareness training on phishing click-through rates," in 2017 IEEE International Conference on Big Data (Big Data), 2017.

[3] A. Gendre, "Facebook Phishing Is Exploding: Why the Social Media Giant is the Latest Phishers' Favorite." [Online]. Available: https://www.vadesecure.com/en/facebook-. [Accessed: 25-May-2021].

[4] A. Gendre, "The art of deception in social media phishing," Vadesecure.com. [Online]. Available: https://www.vadesecure.com/en/the-art-of-deception-in-social-media-phishing/. [Accessed: 25-May-2021].

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

[6] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: state of the art and future challenges," Neural Comput. Appl., vol. 28, no. 12, pp. 3629–3654, 2017.

[7] R. Islam and J. Abawajy, "A multi-tier phishing detection and filtering approach," J. Netw. Comput. Appl., vol. 36, no. 1, pp. 324–335, 2013.

[8] Barracuda Networks, Inc, "Click Thinking Content," Phishline.com. [Online]. Available: https://www.phishline.com/complimentary-content. [Accessed: 25-May-2021].

[9] C. I. Canfield, B. Fischhoff, and A. Davis, "Quantifying phishing susceptibility for detection and behavior decisions," Hum. Factors, vol. 58, no. 8, pp. 1158–1172, 2016.

[10] C. Konradt, A. Schilling, and B. Werners, "Phishing: An economic analysis of cybercrime perpetrators," Comput. Secur., vol. 58, pp. 39–46, 2016.

[11] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, and M. E. Johnson, "Going spear phishing: Exploring embedded training and awareness," IEEE Secur. Priv., vol. 12, no. 1, pp. 28–38, 2014.

[12] D. Goel and A. K. Jain, "Mobile phishing attacks and defence mechanisms: State of art and open research challenges," Comput. Secur., vol. 73, pp. 519–544, 2018.

[13] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study," Comput. Secur., vol. 29, no. 4, pp. 432–445, 2010.

[14] E. Amankwa, M. Loock, and E. Kritzinger, "A conceptual analysis of information security education, information security training and information security awareness definitions," in The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014), 2014.

[15] E. Rader and R. Wash, "Identifying patterns in informal sources of security information," J. cybersecur., p. tyv008, 2015.

[16] E. Trickel, F. Disperati, E. Gustafson, F. Kalantari, M. Mabey, N. Tiwari, Y. Safaei, A. Doupé, G. Vigna, Shell we play a game? CTF-as-a-service for security education, 2017 USENIX Workshop on Advances in Security Education (ASE 17), USENIX Association, Vancouver, BC (2017).

[17] FBI., "Internet Crime Complaint Center (IC3)," Ic3.gov, 2019. [Online]. Available: https://www.ic3.gov/media/2019/190910.aspx. [Accessed: 25-May-2021].

[18] G. Canova et al., "Learn to spot phishing URLs with the android NoPhish app," in Information Security Education Across the Curriculum, Cham: Springer International Publishing, 2015, pp. 87–100.

[19] I. Qabajeh, F. Thabtah, and F. Chiclana, "A recent review of conventional vs. automated cybersecurity anti-phishing techniques," Comput. Sci. Rev., vol. 29, pp. 44–55, 2018.

[20] I. R. A. Hamid and J. H. Abawajy, "An approach for profiling phishing activities," Comput. Secur., vol. 45, pp. 27–41, 2014.

[21] J. Abawajy and T.-H. Kim, "Performance analysis of cyber security awareness delivery methods," in Communications in Computer and Information Science, Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 142–148.

[22] J. Abawajy, "User preference of cyber security awareness delivery methods," Behav. Inf. Technol., vol. 33, no. 3, pp. 237–248, 2014.

[23] J. Abawajy, A. Richard, and Z. A. Aghbari, "Securing websites against homograph attacks," in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Cham: Springer International Publishing, 2018, pp. 47–59.

[24] J. Fruhlinger, "Top cybersecurity facts, figures and statistics," Csoonline.com, 09-Mar-2020. [Online]. Available: https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-. [Accessed: 25-May-2021].

[25] J.-N. Tioh, M. Mina, and D. W. Jacobson, "Cyber security training a survey of serious games in cyber security," in 2017 IEEE Frontiers in Education Conference (FIE), 2017.

[26] K. F. Tschakert and S. Ngamsuriyaroj, "Effectiveness of and user preferences for security awareness training methodologies," Heliyon, vol. 5, no. 6, p. e02010, 2019.

[27] K. L. Chiew, K. S. C. Yong, and C. L. Tan, "A survey of phishing attacks: Their types, vectors and technical approaches," Expert Syst. Appl., vol. 106, pp. 1–20, 2018.

[28] K. RaniSahu and J. Dubey, "A survey on phishing attacks," Int. J. Comput. Appl., vol. 88, no. 10, pp. 42–45, 2014.

[29] M. Baslyman and S. Chiasson, "'Smells Phishy?': An educational game about online phishing scams," in 2016 APWG Symposium on Electronic Crime Research (eCrime), 2016.

[30] M. Fernando and N. A. Arachchilage , "Perth Why Johnny can't rely on anti-phishing educational interventions? Why Johnny can't rely on anti-phishing educational interventions to protect himself against contemporary phishing attacks?", Australasian Conference on Information Systems, 2019.

[31] M. M. Al-Daeef, N. Basir, and M. M. Saudi, "Security awareness training: A review," in Lecture Notes in Engineering and Computer

Science: Proceedings of The World Congress on Engineering 2017. International Association of Engineers (IAENG), Newswood Limited, 446–451, 2017.

[32] M. Volkamer et al., "Developing and evaluating a five-minute phishing awareness video," in Trust, Privacy and Security in Digital Business, Cham: Springer International Publishing, 2018, pp. 119–134.

[33] N. A. G. Arachchilage, S. Love, and K. Beznosov, "Phishing threat avoidance behaviour: An empirical investigation," Comput. Human Behav., vol. 60, pp. 185–197, 2016.

[34] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching Johnny not to fall for phish," ACM Trans. Internet Technol., vol. 10, no. 2, pp. 1–31, 2010.

[35] Proofpoint, "Threat Report: 2020 State of the Phish Report." [Online]. Available: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish. [Accessed: 25-May-2021].

[36] R. M. Mohammad, F. Thabtah, and L. McCluskey, "Tutorial and critical analysis of phishing websites methods," Comput. Sci. Rev., vol. 17, pp. 1–24, 2015.

[37] R. N. Landers and C. M. Reddock, "A meta-analytic investigation of objective learner control in web-based instruction," J. Bus. Psychol., vol. 32, no. 4, pp. 455–478, 2017.

[38] R. Valecha, A. Gonzalez, J. Mock, E. J. Golob, and H. Raghav Rao, "Investigating phishing susceptibility—an analysis of neural measures," in Information Systems and Neuroscience, Cham: Springer International Publishing, 2020, pp. 111–119.

[39] R. Wash and M. M. Cooper, "Who provides phishing training?: Facts, stories, and people like me," in Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18, 2018.

[40] S. Abraham and I. Chengalur-Smith, "Evaluating the effectiveness of learner-controlled information security training," Comput. Secur., vol. 87, no. 101586, p. 101586, 2019.

[41] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions," in Proceedings of the 28th international conference on Human factors in computing systems - CHI '10, 2010.

[42] S. Stockhardt et al., "Teaching Phishing-Security: Which Way is Best?," in ICT Systems Security and Privacy Protection, Cham: Springer International Publishing, 2016, pp. 135–149.

[43] V. Suganya, "A review on phishing attacks and various anti phishing techniques," Int. J. Comput. Appl., vol. 139, no. 1, pp. 20–23, 2016.

[44] Z. A. Wen, Z. Lin, R. Chen, and E. Andersen, "What.Hack: Engaging anti-phishing training through a role-playing phishing simulation game," in Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19, 2019.