CHALLENGES OF THE SUCCESS OF CYBERSECURITY TRAINING PROGRAMS

Melad Al-Daeef *

Faculty of Information Technology, Elmergib University, Al-Khoms, Libya
** Corresponding author: mmaldaeef@elmergib.edu.ly*

ABSTRACT

Internet-based attacks issue still terrifies the Internet community including the individuals and employees at public and private organizations. Many solutions were proposed to protect the Internet users against cybersecurity attacks. Most of the solutions target the technical side of information systems. Attackers, therefore, still able to bypass technical-based solutions through the human unawareness factor. Therefore, organizations have to implement effective training programs to enhance their employees' security awareness and influence them to comply with security rules and policies. The problem which still exist is the challenges that confront the implementation process of effective security training programs. That is why, security training challenges need to be analyzed to highlight the factors that limit the success of training programs. In this paper, security training challenges are categorized into three types based on which aspect they occur and cause impacts. The challenges are categorized as; organization-related challenges, trainees-related challenges, and training program-related challenges.

Keywords: awareness, information security, phishing, training.

1. INTRODUCTION

Security awareness is a critical issue that the organizations always concern about. Organizations must improve their employees' security awareness to avoid security threats that may be caused by employees' misbehavior, these incidents may occur accidentally or deliberately. Whatever the reason, cybersecurity threats will eventually cause big financial and/or reputational losses. Phishing is the most known example of cyber threats in which, the attackers try to utilize the human un-awareness factor to bypass automated (computer-based) security countermeasures.

Many reports show that phishing is in obvious increase. Anti-Phishing Working Group APWG [1] show that the number of recent phishing attacks has more than doubled since early 2020, while the APWG has observed a number between 68,000 and 94,000 attacks per month. In July 2021for example, APWG has observed a number of 260,642 attacks. This number was the highest monthly count recorded in APWG's reporting history.

Besides the phishing, many of security gaps from which the Internet may threatened. Unawareness factor may lead a user to be fall prey for an attack.

In general, countermeasures of cyber threats classified into two categories, technical and non-technical solutions. The technical ones are implemented to mitigate the security breaches that caused by a failure in the software and/or hardware of information system. The non-technical solutions, on the other side, are applied to mitigate the security breaches that caused by the people who interact with the information system. Researchers claim that, relying only on the technical aspect of solutions is insufficient to protect the information systems, such solutions need to be complemented by efficient non-technical ones. A considerable concern should be directed to human awareness factor to improve the cyber security countermeasures [2][3][4][5]. This study, therefore, focuses on the challenges to security awareness factor and security training programs as a non-technical solution that used to mitigate cyber security threats.

2. DEFINITION OF SECURITY AWARENESS

Security awareness has received different definitions to meet a variety of security requirements. According to Information Security Forum (ISF) in [6], the security awareness was identified as a continual process of learning by which, the trainees understand the information security issues, the organizational security aims, and the trainees' responsibilities to achieve these security aims. Another security awareness definition was stated in [7] "a state where users in an organization are aware of and ideally committed to their security mission". Based on the research in [8], two aspects compromise the security awareness; 1st, appropriate knowledge must be accurately and timely presented to targeted trainees; 2nd, the presented knowledge should impact individuals' behavior. If one of these aspects was has missed, the other one, therefore, becomes useless. The researchers [8] have defined security awareness as "the effort to impart the knowledge about information security to the degree that influence users' behavior, thus they conform to applied security policies". Three aspects of security awareness were highlighted in the above security awareness definitions, they are; ongoing or continual process, knowledge delivery method, and trainees' behavior impact. However, these earlier definitions have left out an important element in the knowledge acquiring process, which is the gradation concept.

Based on the Adaptive Control of Thought-Rational (ACT-R) theory [9], the knowledge and values are gradually acquired and learned through practice. Human brain keeps statistics on the frequency, recency, and utility of knowledge components [10]. Based on these characteristics of human brain, researchers in [4] have identified the security awareness as the knowledge that gradually acquired through a continuous and updated attractive training method that influences the trainees' behavior.

3. REASONS OF THE SUCCESS OF CYBER SECURITY ATTACKS

Researchers in many studies have highlighted the reasons of the success of cybersecurity attacks, the most well-known of these reasons are presented in the following;

a. Many of Internet users consider the security just a secondary and less important task compared to their primary aim of Internet browsing [11].

b. Users' inattention, ignorance and non-compliance with security policies [12][13].

c. Users in many cases do not have time to attend ongoing and/or long term security training programs, or even they do not have time to implement trained security rules [14][15].

d. The failure to design efficient training program and identify its objectives [5][16].

e. Users' overconfidence leads to wrong thinking that they are aware enough to detect security threats [17][18].

f. The failure to implement motivation factors and/or sanctions to enforce the compliance with security policies in organizations [19].

Researchers, therefore, recommend the solutions that can be applied at the non-technical (human) layer of information systems. Security training awareness is the well-known applicable and efficient solution. The training approach has proved its usefulness to support the performance of automated (computer-based) information security systems [4][20].

4. CHALLENGES TO SECURITY TRAINING IMPLEMENTATION

The introduction in this research has highlighted the importance of human awareness in the success of information security solutions and, thus, reduce the adverse effects of potential security threats. To enhance the security awareness of the employees, many training programs with a variety of training methods have been implemented [3][21][22]. Yet, each of these training methods has its own limitations to improve the trainees' ability to detect information security threats [23][24]. To achieve the desired goals of security training programs, these programs must be properly designed, presented and led. They must fulfill the organizations' missions to influence the trainees' security-related behavior [25][26]. However, there are many challenges that must be defeated to design successful security training programs. Researchers in [12] revealed that the security training practices and security guidelines in many cases are presented at a conceptual level with no empirical evidence and validity. In addition, these practices are usually implemented in a common format (one-size-fits-all) with the omission of environmental differences where they are applied. The researchers in [12] have also underlined three challenges that limit the success of security training programs. These and some other challenges are discussed below;

1. The lack of motivational factors is one of the challenges that limit the success of information security training and awareness programs. It is always recommended by many researchers to investigate employees' behavior and motivate them to understand the potential risks, and to attend security training programs. Attending training programs is important factor in increasing the awareness of trainees and important to motivate them to learn, and thus show a positive security behavior. As a consequence they comply with information security policies and perform their duties with greater

caution [2][5][12][27]. Several studies in the literature have reported that rewards are one of the effective factors for achieving the goals of security training programs, the most prominent of which is to motivate the employees to comply with security procedures and policies [13][16][28]. Rewards can be awarded in tangible and/or intangible forms. On the other hand, other researchers argue that, rewards can negatively affect the employees' intention to comply with security policies especially if this compliance causes some kind of inconvenience. An example of this inconvenience is the extra time required to complete a task when complying with security rules, this will most likely make the employees show improper security behavior [15][19]. Researchers also suggest that fear and perceived importance can motivate employees to comply with security rules. They suggest that the managers and security admins must announce the importance of compliance with security rules, and should clearly define rewards and/or penalties to get employees to adhere with security rules [19].

2. Competition for employee attention is another challenge that limits the success of security training programs. To overcome this challenge, five factors have been considered in [12] and they are discussed in below;

   1st factor, many methods to deliver the security training materials must be practiced to get the attention of the trainees [12], the performance of the trainees is usually affected by the training delivery method [27]. In [29], four of the most widely used training delivery methods are discussed, namely, E-learning, game-based training, video-based training, and instructor-led training. In several studies, researchers have compared the effectiveness of training delivery methods, and detailed results from the comparisons are presented in [30][31]. A higher level of training efficiency can be achieved by combining different methods rather than relying on just one method, and the decision on which method to choose, should always be determined based on the content of training program [27]. Furthermore, it is desirable that, for the training exercise to have a lasting impact, employees or trainees should be reminded frequently of the training materials. Security administrators, therefore, should make clear plans for when and how to remind trainees [22].

   2nd factor, shortening the content of security training program is important to increase its efficiency [12]. Researchers in some studies argue that, instructor-based training should be as short as possible for the purpose of memorizing and increasing program efficiency [32] as reported in [23]. With regard to the content of security training program, it must, in addition, be compatible with the training delivery method [2][27], and it must be correct, up-to-date, relevant and appropriate for intended trainees to positively influence their performance and behavior [26].

   3rd factor, develop the security training program to target the employees who deal with sensitive information. The process of content design must consider the targeted participants' level of awareness about the information security issues [12][27]. It’s an important matter to monitor and motivate employees who deal with sensitive information to protect it. Although the employees know the value of information and resources they deal with. In some cases, however, they may act in a way that harms that information even if their act was not motivated by malicious intent [33].

4th factor, training delivery methods must balance getting trainees’ attention and flooding them with training information that to avoid a situation in which they get confused. One of the most potential security threats is the trainees' lack of attention to cybersecurity standards and rules. While designing of security programs and choosing the methods to deliver training, program administrators should focus on how to enhance individual willingness not only to participate in the training program, but also to practice the trained lessons in their daily tasks and make it as a sustainable habit [4][12][27].

The 5th factor, investigation of successful security training programs for organizations with similar risks. This helps alleviate the problem of trainees’ limited time and attention [12][34]. Investigating the types of threat gives a clear picture of the threats faced by other organizations [29], and thus, security administrators can easily design efficient security training programs. However, training program designers must not forget that different organizations have different needs. This is an important consideration for building a more efficient and cost-effective security awareness program that addresses the specific needs of the organization [27].

3. The difficulty of measuring the effectiveness of training programs. Although there is a consensus that a well-practiced training experience has an exemplary effect on the trainees, there still a critical issue which is the ability to measure the overall efficiency of the training program[12][35]. Some of the actions that taken to overcome this challenge are;

   a. The effectiveness of security training programs can be measured by determining the security awareness and knowledge retention with the consideration of the diversity of implemented training methods, it should be noted that, each of training delivery methods has its own advantages and disadvantages [30][31].

   b. The number of reported security incidents can also be used to measure the effectiveness of security training programs. Increased employee awareness usually results in reducing the rate of such reported incidents since the level of security awareness is inversely proportional to the number of reported incidents [29][31].

   c. Testing the level of security knowledge of the trainees before and after attending the training experiment is an important procedure to know their opinions about the training program [3][12]. Trainers must assess the knowledge level of the trainees before and after the training experiment [27]. Knowing the trainees’ opinion is an important factor in improving security procedures. This adds a point of strength and effectiveness to the training program [36]. Trainees' opinions and feedback of can be obtained in several ways, the questionnaire is one of such ways. However, other training methods such as the instructor-based method allow the direct feedback on the performance of the trainees [23][37].

d. Carrying out simulated attacks on the organization's network, for example by sending fake email messages to test whether the security rules are in place or not. It is an important step to evaluate the security procedures for discovering any vulnerabilities, thus, avoiding possible incidents [12][28]. These assessments and measures are also important to collect the necessary information and also to know the resources required to develop optimal training experiments, thus, meeting the desired level of security awareness [27][37].

4. Another challenge which limiting the efficiency of security training programs is the knowledge retention factor. There is no doubt about the limitation of human memory in retaining the acquired knowledge for a long time, people simply forget facts and details [29]. Several studies have examined the lasting impact of security training programs. However, it is very difficult to agree on the ideal retention time of security knowledge. Many studies have assessed the lasting effect of security knowledge based on unequal time periods. Some have evaluated the training effect immediately after the end of training program such as in [22]. Others have evaluated it after time periods that span over 1 month as in [38][39], 45 days as in [40], 8 weeks as in [41], 5 months as in [42]. Researchers in [22] found that after six and eight months, participants' skills were no longer much better than they were before they attended the training program. Accordingly, it is not recommended to always rely on the knowledge retention factor to implement security procedures, it is advisable to periodically remind the employees of the security rules and policies that they must adhere to. The period intervals of these reminders must be precisely specified.

5. The total cost of training programs is another challenge upon which the success of the training program depends. Organizations always pay attention to the budget and try to implement the resources that provide security standards at the lowest costs [43]. The expenses for security-related requirements must be constantly covered by the organization's top management. However, this does not mean that once the money is spent the training program will success. The real estimation of the cost of the training program is one of the factors of its success [27]. Therefore, it is recommended to measure the effectiveness of the training program to know if it is worth its cost.

6. Another challenge is the organization ability to fairly treat its employees, especially those who intended to be aware about security rules.

5. CLASSIFYING OF SECURITY TRAINING CHALLENGES

Despite the numerous researches in the field of security training, there are many challenges that limit the effectiveness of training programs. The most known challenges were discussed in the previous section. The literature shows that, an organization may face different types of challenges when developing a security training program. Researchers in [28], for example, have proposed nine initiatives to defeat security challenges. In this study, we recommend analyzing the nature, effects, and vectors of security training challenges in order to overcome their negative impacts. These analyses are necessary to implement the appropriate initiatives to address the real challenges faced by the organization. Below, the challenges to security training programs are categorized based on the aspect in which they occur and cause their effects;

1. Management / Organization -Related Challenges

The management support is a very important factor in defining the main objectives of a security training program. Enterprise security administrators must identify and analyze the potential threats, especially those that arise from humans, that must mitigate their adverse effects. The analysis of the challenge lead to a good design of the training program, thus, clearly defining its objectives. Management support gives a clear picture of the current state of the organization and availability of the resources required to conduct a security training program. These resources include but not limited to, the budget, premises and machines. The management support is also required to schedule the program time based on the trainees' duties and availability.

2. Program-Related Challenges

Many challenges affect the effectiveness of security training programs, most obvious challenges are outlined here. 1st, the designers of training program need to choose the appropriate training delivery method based on many factors such as the number of trainees, the nature of threats, and available resources. Moreover, the program designers must consider that training material greatly influence the choice of delivery method. Both of the training material and the training delivery method will therefore affect the knowledge retention factor that must be extremely considered when the training program is designed. The knowledge retention of employees should be tested and evaluated periodically, and they should be periodically reminded of the training material. These reminder intervals must be fine-tuned based on many factors such as when the training material should be reviewed and updated.

3. Trainees-Related Challenges

In this context, several challenges may have a negative impact on the effectiveness of the training programs. One of such challenges is targeting the right group of employees. The employees must participate in an appropriate training experiment in terms of training materials, delivery methods, time and course duration. Another challenge in this context is the trainees' intention to attend the training experiment. Some trainees may be enrolled in and attend the training program; however, they may not reach the desired goal of awareness, nor be concerned with the knowledge they acquire. Moreover, even in cases where employees receive sufficient knowledge and are supposed to be more aware, they may show a negative behavior towards security policies and rules. This behavior may be caused by the employees' overconfidence that they knowledgeable and aware enough to protect the information system without adhering to security rules. This may also happen if employees do not realize the importance of security rules for the organization. Or sometimes due to employees' deliberate ignorance and neglect of security rules. In some cases, employees may intentionally bypass security rules to get duties done quickly and easily. Other employees may show negative behavior due to the stress at work and/or the external environment. In other cases, employees may see or feel that their managers are treating them unfairly, thus, they deliberately ignore security rules as a retaliatory reaction. In addition, the negative behavior of employees may occur in some cases due to unintended errors.

Whatever the reasons of the negative behavior of employees towards security rules and policies, the managers must identify and analyze these reasons. They also must find a way to force the compliance to security policies. The managers can use the rewards and/or punishments to ensure a satisfactory level of security policies adherence. They in some cases may need to allow or engage the employees in making the security-related decisions.

6. CONCLUSION

This paper has discussed the challenges that limit the success of security training programs. These challenges differ in nature, causes, effect and also in the program aspect in which they occur. The literature shows that, there is no one-size-fits-all solution, every organization (targeted trainees' group) has a situation that is different in some way from the others. Therefore, organizations should customize the training programs to meet their own needs. This paper recommends the analyze and classify of challenges that the security training program may face. Such process will help in the classification of security training challenges, this will be useful for the organizations to perform effective training programs. The investigation presented in this paper shows that security training challenges fall into three main categories, namely: challenges related to the organization, challenges related to the training program, and challenges related to trainees. In future, each of these challenges can be further investigated to come out with more specific solutions relating to each "type" of these challenges.

REFERENCES

[1] Anti-Phishing Working Group, “Phishing Activity Trends Report 3rd Quarter,” no. November, pp. 1–9, 2021.

[2] R. Rohan, S. Funilkul, D. Pal, and W. Chutimaskul, “Understanding of Human Factors in Cybersecurity: A Systematic Literature Review,” no. April 2022, pp. 133–140, 2022, doi: 10.1109/compe53109.2021.9752358.

[3] K. F. Tschakert and S. Ngamsuriyaroj, “Effectiveness of and user preferences for security awareness training methodologies,” *Heliyon*, vol. 5, no. 6, p. e02010, 2019, doi: 10.1016/j.heliyon.2019.e02010.

[4] M. M. Al-Daeef, N. Basir, and M. M. Saudi, “Security awareness training: A review,” in *Lecture Notes in Engineering and Computer Science*, 2017, vol. 2229.

[5] H. W. Glaspie and W. Karwowski, “Human factors in information security culture: A literature review,” *Adv. Intell. Syst. Comput.*, vol. 593, pp. 267–280, 2018, doi: 10.1007/978-3-319-60585-2_25.

[6] “The Standard of Good Practice for Information Security.” 2007.

[7] M. T. Siponen, “A conceptual foundation for organizational information security awareness A conceptual foundation for organizational information security awareness,” vol. 8, no. 1, pp. 31–41, 2006.

[8] M. Wolf, D. Haworth, and L. Pietron, “Measuring An Information Security Awareness Program,” *Rev. Bus. Inf. Syst.*, vol. 15, no. 3, pp. 9–22, 2011.

[9] J. R. Anderson and C. D. Schunn, “Implications of the ACT-R Learning Theory : No Magic Bullets Implications of the ACT-R Learning Theory : No Magic Bullets Department of Psychology,” vol. 5, pp. 1–27, 2000.

[10] C. Anderson, J. R., Matessa, M., & Lebiere, “ACT-R: A theory of higher level cognition and its relation to visual attention,” *Human-computer interaction*, vol. 12, no. 4. pp. 439–462, 1997.

[11] P. Rajivan and C. Gonzalez, “Creative persuasion: A study on adversarial behaviors and strategies in phishing attacks,” *Front. Psychol.*, vol. 9, no. FEB, pp. 1–14, 2018, doi: 10.3389/fpsyg.2018.00135.

[12] M. Alshaikh, S. B. Maynard, A. Ahmad, and S. Chang, “An exploratory study of current information security training and awareness practices in organizations,” *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 2018-Janua, pp. 5085–5094, 2018, doi: 10.24251/hicss.2018.635.

[13] Angraini, R. A. Alias, and Okfalisa, “A model of information security policy compliance for public universities: A conceptual model,” *Adv. Intell. Syst. Comput.*, vol. 1073, pp. 810–818, 2020, doi: 10.1007/978-3-030-33582-3_76.

[14] S. W. Schuetz, P. B. Lowry, and J. B. Thatcher, “Defending against spear-phishing: motivating users through fear appeal manipulations Technology: New Forms and Development Structures View project Security View project,” pp. 0–11, 2016, [Online]. Available: https://www.clemson.edu/business/about/profiles/?userid=JTHATCH

[15] A. Vance, M. Siponen, and S. Pahnila, “Motivating IS security compliance: Insights from Habit and Protection Motivation Theory,” *Inf. Manag.*, vol. 49, no. 3–4, pp. 190–198, 2012, doi: 10.1016/j.im.2012.04.002.

[16] G. Dhillon, Y. Yakimini, A. Talib, and W. N. Picoto, “The Mediating Role of Psychological Empowerment in Information Security Compliance Intentions,” vol. 21, pp. 152–174, 2020, doi: 10.17705/1jais.00595.

[17] A. Alnajim and M. Munro, “An evaluation of users’ tips effectiveness for phishing websites detection,” *3rd Int. Conf. Digit. Inf. Manag. ICDIM 2008*, pp. 63–68, 2008, doi: 10.1109/ICDIM.2008.4746717.

[18] 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, doi: 10.1145/1754393.1754396.

[19] M. Siponen, M. Adam Mahmood, and S. Pahnila, “Employees’ adherence to information security policies: An exploratory field study,” *Inf. Manag.*, vol. 51, no. 2, pp. 217–224, 2014, doi: 10.1016/j.im.2013.08.006.

[20] F. A. Aloul, “The Need for Effective Information Security Awareness,” *J. Adv. Inf. Technol.*, vol. 3, no. 3, pp. 176–183, 2012, doi: 10.4304/jait.3.3.176-183.

[21] A. Kunz, M. Volkamer, S. Stockhardt, S. Palberg, T. Lottermann, and E. Piegert, “NoPhish: Evaluation of a web application that teaches people being aware of phishing attacks,” *Lect. Notes Informatics (LNI), Proc. - Ser. Gesellschaft fur Inform.*, vol. P-259, pp. 509–518, 2016, doi: 10.5445/IR/1000081981.

[22] M. V. Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Mattia Mossano, Reyhan Duezguen, Bettina Lofthouse, Tatiana von Landesberger, “An investigation of phishing awareness and education over time: When and how to best remind users.” 2020.

[23] S. Stockhardt *et al.*, “Teaching phishing-security: Which way is best?,” *IFIP Adv. Inf. Commun. Technol.*, vol.

471, pp. 135–149, 2016, doi: 10.1007/978-3-319-33630-5_10.

[24] L. Jaeger, “Information Security Awareness: Literature Review and Integrative Framework,” vol. 9, no. 3, pp. 4703–4712, 2018, doi: 10.24251/HICSS.2018.593.

[25] M. Wilson and J. Hash, “Building an Information Architecture Checklist,” *Organization*, vol. 2, no. 2, pp. 25–42, 2002, doi: 10.1109/IEMBS.2010.5627684.

[26] P. Model, M. Wilson, and P. Bowen, “NIST Special Publication 800-16 (Draft),” vol. 1, 2009.

[27] A. Ghazvini and Z. Shukur, “Awareness Training Transfer and Information Security Content Development for Healthcare Industry,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 5, pp. 361–370, 2016, doi: 10.14569/ijacsa.2016.070549.

[28] T. Security, “Information Security Practices in Organizations : A Literature Review on Challenges and Related Measures”.

[29] B. J. Guimaraes and M. Sc, “Information Security Awareness : Learning for Effectiveness,” 2021.

[30] P. Kim and J. V Homan, “Measuring the Effectiveness of Information Security Training: a Comparative Analysis of Computer-Based Training and Instructor-Based Training,” *Issues Inf. Syst.*, vol. 13, no. 1, pp. 215–224, 2012, doi: 10.48009/1_iis_2012_215-224.

[31] J. Abawajy, “User preference of cyber security awareness delivery methods,” *Behav. Inf. Technol.*, vol. 33, no. 3, pp. 237–248, 2014, doi: 10.1080/0144929X.2012.708787.

[32] R. Schmid, “‘Entwickeln einer Awareness-Kampagne für einen sicheren Umgang mit dem Internet an mittelgrossen Berufs- oder Maturitaetsschulen,’” Hochschule Luzern, Wirtschaft, 2010. [Online]. Available: http://www.zanzara.ch/download/Masterarbeit_Awareness_mit_Logo_klein.pdf

[33] R. Willison and M. Warkentin, “Beyond deterrence: An expanded view of employee computer abuse,” *MIS Q. Manag. Inf. Syst.*, vol. 37, no. 1, pp. 1–20, 2013, doi: 10.25300/MISQ/2013/37.1.01.

[34] P. Kumaraguru *et al.*, “Getting users to pay attention to anti-phishing education,” *Proc. anti-phishing Work. groups 2nd Annu. eCrime Res. summit - eCrime ’07*, pp. 70–81, 2007, doi: 10.1145/1299015.1299022.

[35] A. Da Veiga, “An information security training and awareness approach (ISTAAP) to instil an information security-positive culture,” *Proc. 9th Int. Symp. Hum. Asp. Inf. Secur. Assur. HAISA 2015*, no. Haisa, pp. 95–107, 2015.

[36] N. Waly, R. Tassabehji, and M. Kamala, “Improving organisational information security management: The impact of training and awareness,” *Proc. 14th IEEE Int. Conf. High Perform. Comput. Commun. HPCC-2012 - 9th IEEE Int. Conf. Embed. Softw. Syst. ICESS-2012*, pp. 1270–1275, 2012, doi: 10.1109/HPCC.2012.187.

[37] N. A. Bakar, M. Mohd, and R. Sulaiman, “Information leakage preventive training,” *Proc. 2017 6th Int. Conf. Electr. Eng. Informatics Sustain. Soc. Through Digit. Innov. ICEEI 2017*, vol. 2017-Novem, pp. 1–6, 2018, doi: 10.1109/ICEEI.2017.8312403.

[38] E. J. F. M. Custers, “Long-term retention of basic science knowledge: A review study,” *Adv. Heal. Sci. Educ.*, vol. 15, no. 1, pp. 109–128, 2010, doi: 10.1007/s10459-008-9101-y.

[39] P. Kumaraguru *et al.*, “School of Phish : A Real-World Evaluation of Anti-Phishing Training Categories and Subject Descriptors,” *Proc. 5th Symp. Usable Priv. Secur. - SOUPS ’09*, p. 12, 2009, doi: 10.1145/1572532.1572536.

[40] T. Zhang, “Knowledge Expiration in Security Awareness Training,” *Annu. ADFSL Conf. Digit. Forensics, Secur. Law*, no. c, pp. 197–212, 2018.

[41] M. Volkamer *et al.*, “Developing and evaluating a five minute phishing awareness video,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11033 LNCS, pp. 119–134, 2018, doi: 10.1007/978-3-319-98385-1_9.

[42] G. Canova, M. Volkamer, C. Bergmann, and B. Reinheimer, “NoPhish App Evaluation: Lab and Retention Study,” 2015, doi: 10.14722/usec.2015.23009.

[43] A. Jayatilaka *et al.*, “Evaluation of Security Training and Awareness Programs: Review of Current Practices and Guideline,” pp. 1–12, 2021, [Online]. Available: http://arxiv.org/abs/2112.06356