Human and Cognitive factors involved in Phishing detection. A literature review.

1st Diana Arévalo
CERT Radical,
Grupo Radical
Quito, Ecuador
diana.arevalo@gruporadical.com

2nd Darío Valarezo
Department of Computer Sciences
Universidad de las Fuerzas Armadas
Sangolquí, Ecuador
divalarezo@espe.edu.ec

3rd Walter Fuertes
Department of Computer Sciences
Universidad de las Fuerzas Armadas
Sangolquí, Ecuador
wmfuertes@espe.edu.ec

4th María Fernanda Cazares
IDEIAGEOCA
Universidad Politécnica Salesiana
Cuenca 010102, Ecuador
mcazares@ups.edu.ec

5th Roberto O. Andrade
Facultad de Ingeniería en Sistemas
Escuela Politécnica Nacional
Quito 170525, Ecuador
roberto.andrade@epn.edu.ec

6th Mayra Macas
Department of Computer Sciences
Universidad de las Fuerzas Armadas ESPE
Sangolquí P.O. Box 17-15-231B, Ecuador
mmacas@espe.edu.ec

***Abstract*—Human and cognitive factors considerably influence social engineering attacks. Cybercriminals take advantage of the innocence, carelessness, stress, lack of knowledge, and other aspects that make human beings vulnerable. Also, there exists difficulty for users to identify an email with phishing. However, the causes and solutions are not only technological; they also depend on human perception. Within this context, in this paper, we perform a systematic literature review using the PRISMA guidelines of the recent studies applying security and cognitive psychology, aiming to identify the human and cognitive factors that are part of a Phishing attack. The main findings of this research are focused on developing future research in cybersecurity, which we believe should go in hand with human cognitive and psychological factors.**

***Index Terms*—Cognitive security; cognitive psychology; phishing; human factors; risk perception**

I. Introduction

Currently, the most common method of gathering information is using social engineering attacks through manipulative social skills to convince others to perform various actions [1] [2]. Among the most widespread social engineering attacks are phishing attacks [3], [4]. Such attacks target users who are not knowledgeable about social engineering and Internet security [5]. The most common methods and techniques used for phishing are emails, chats, or websites and one of the main reasons this type of attack continues to grow is the lack of knowledge of users [6], [7]. Compared to the first quarter of 2021, the Anti-Phishing Working Group's (APWG) Phishing Activity Trends (PDF) report recorded 1,025,968 phishing attacks up to March 2022 [8]. In the entire technological sector, phishing attacks were the top target in Q1, particularly social networks (21.5%), webmail/online services (5.5%), e-commerce (1.9%), and cloud storage [9].

The increasing sophistication of phishing attacks causes billions of dollars in financial losses, losses of intellectual property, and reputational damage to organizations [10]. This type of cyber-attack is often successful because users are unaware of their vulnerabilities or are unable to understand the latent risks [4]. The 'human factor' has been recognized as the weakest and darkest link in creating safe and secure digital environments [11]. Recent studies have found that the feature called 'phishing susceptibility' (i.e., the likelihood of being phished) is closely related to the personality traits of individuals [3]. Therefore, changing the way that a person thinks with respect to social engineering is key for identifying and defending against such attacks [12]. To that end, cognitive sciences can enhance and draw light to the cognitive processes, which can help security analysts to establish actions in less time and more efficiently within cybersecurity operations [13].

This paper presents a systematic literature review (SLR) about the cognitive factors and the techniques and tools used in cognitive security against phishing attacks. The followed methodology is based on the PRISMA guidelines [14]. The results provide important insights to researchers regarding the cognitive factors that are relevant when detecting phishing attacks. Furthermore, the current techniques and tools leveraging security and cognitive psychology are presented, where the human factor is directly involved in the detection of phishing.

The remainder of the article is organized as follows: Section 2 provides back-ground information. In Section 3, we outline the SLR procedure, while in Section 4, we discuss and analyze the significance of the generated results in terms of the explored research questions. Finally, we provide concluding re-marks and outline future research directions in Section 5.

II. Background

A. Cognitive Security

Cognitive security leverages the generalization and abstraction capabilities that allow humans to solve problems and analyze the potential impact of decisions made [13]. It has become an important term in cybersecurity in recent years. Andrade R. and Torres J. have defined it as the ability to generate cognition for efficient decision-making in real-time by a human or a

979-8-3503-2759-5/23/$31.00 ©2023 IEEE
DOI 10.1109/CSCE60160.2023.00105

computer system, based on the perception of cybersecurity that the computer system generates [15]. Cognitive security generally refers to the practices, methodologies, and efforts to defend against social engineering attempts. However, within the cyber security context, it regards explicitly the application of artificial intelligence and machine learning technologies that rely on human cognition to perform security threat detection [16]. In order to address security challenges, new cognition-inspired security architectures that emphasize dynamic and autonomous trust management have been proposed. [17].

B. Cognitive Factors

Cognitive factors refer to the person's characteristics that affect performance and learning. These factors serve to modulate performance so that it can improve or decrease [18]. Simon [19] mentions that the cognitive component of people is made up of certain elements that act on the behavior of beings and are related to decision-making and problem-solving, such as perception, attention, and memory.

C. Phishing attacks

Phishing attacks are the most common method of cybercrime that convinces people to provide confidential information, such as account IDs, passwords, and bank details, employing emails, instant messages, and phone calls [20]. Phishing emails are a significant problem related to fraud and exploitation and can harm health, causing depression and even suicide [21] [22]. Table I summarizes recent research studies dealing with human factors in the context of phishing.

The user's perception, understanding, and risk projection are not so easy to automate; this is due to the lack of consolidation of human factors-related attributes, the application of theoretical frameworks, and the lack of in-depth qualitative studies. Desolda et al. [4] conclude that the most vulnerable human factors exploited by attackers during phishing scams are lack of knowledge, resources, awareness, norms, and complacency. Moreover, Jeong et al. [11] present a study examining human factors' subjective and complex nature in cybersecurity. Andrade et al. [34] present a SLR regarding the security incident handling process to identify guidelines published by organizations, and they analyze the contribution of cognitive security to improve the cognitive skills.

III. Methodology

This study follows the PRISMA guidelines, which is relevant for systematic literature reviews as mixed methods that include quantitative and qualitative analyses, and is based on the next four research questions:

RQ1. What are the techniques involving the human factor in phishing detection?.

RQ2. What are the new Cognitive Security techniques and tools in Phishing detection?.

RQ3. How can Cognitive Psychology be applied to Phishing detection?.

RQ4. What is the human perception of risk in the face of social engineering attacks?

Figure 1 depicts the four phases of the PRISMA methodology used in this work. Regarding the inclusion and exclusion criteria, the following has been defined: articles that were not written in English and that were not published between 2016 and 2022 were excluded. This temporal cut-off enabled us to find essential studies that determine users' risk perception against Phishing-type social engineering attacks. For this purpose, the following inclusion criteria were applied:

- Articles whose content reflects users' behavior and risk perception in the face of Phishing attacks in any context.
- Articles whose content concerns current security methods/tools and Cognitive Psychology approaches where the human factor is directly involved.
- Articles published in journals or conference proceedings of Q3 quartile or higher.

We conduct the search process in the following scientific databases/indices:

- ACM Digital Library (https://dl.acm.org/)
- IEEE Digital Library (https://ieeexplore.ieee.org/)
- Scopus (http://www.scopus.com/)
- Springer (https://www.springer.com/)

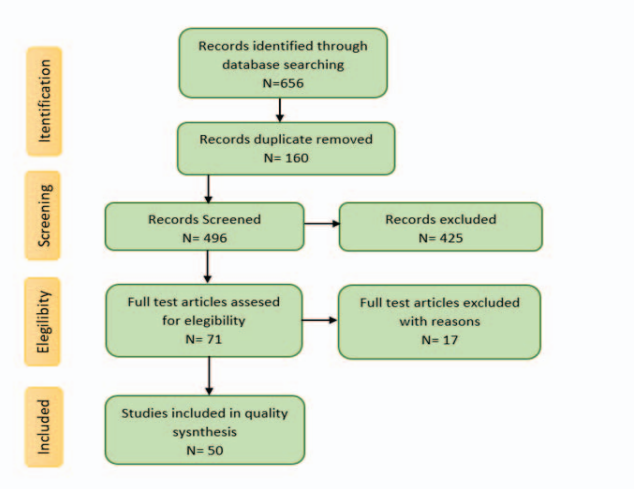

Fig. 1. SRL process applying the PRISMA methodology

As previously mentioned, we considered journal articles and proceedings from 2016 and later. The search keywords were: cognitive security, cognitive psychology, phishing, human factor, and risk perception. We applied the following search string as the primary search string:(((Cognitive security AND phishing) OR human factors)) AND (Social engineering attacks AND Cognitive security) AND ((Cognitive security AND cognitive psychology) AND phishing) AND ((Cognitive security AND phishing) AND human factors OR risk perception). As a result, we discovered 656 articles. We then applied the inclusion and exclusion criteria to preselect 67 of them. Subsequently, we read the title, abstract, development process, and conclusions to fine-tune and finalize the selection.

Regarding the publication sources, we selected nine papers published in conference proceedings. The remaining studies

TABLE I
RECENT RESEARCH STUDIES DEAL WITH HUMAN FACTORS IN DETECTING PHISHING ATTACKS.

Cognitive factors	Fields of application	Technical Content	Reference	Year
Human behavior	Phishing	Application for detecting phishing attacks based on human behavior when exposed to a fake website.	[23]	2017
Decision making	Social Phishing	Socio-cognitive and computational model.	[24]	2017
Susceptibility, authority, urgency and risk perception	Phishing	Survey application exploring phishing emails with varying degrees of authority, urgency signals, and risk signals.	[25]	2020
Susceptibility, detection and behavioral decisions	Phishing	Use of signal detection theory.	[26]	2016
Susceptibility	Phishing	Applying a Phishing Email Suspicion Test (PEST) and developing a laboratory task to assess the cognitive mechanisms of phishing detection.	[21]	2020
Human behavior	Phishing	A proof-of-concept model based on the ACT-R cognitive architecture.	[27]	2017
Susceptibility	Phishing	A Model of suspicion, cognition and automaticity	[28]	2016
Susceptibility	Phishing	Developing a model based on the probability of elaboration. Data were collected through direct observations and self-reported questionnaires.	[29]	2019
Decision making (trust or distrust)	Phishing	Devising an experimental protocol through the application of a questionnaire.	[30]	2021
Susceptibility, certainty and tension	Phishing	Using an integrated perspective of emotion based on the Affective Information Model.	[10]	2019
Susceptibility to scarcity and reciprocity	Spear Phishing	Conducting a controlled experiment examining young and old Internet users.	[31]	2017
Susceptibility, impulsivity	Phishing	Performing simulated phishing experiments.	[32]	2021
Susceptibility	Phishing	Developing an instance-based learning (IBL) model for predicting user behavior.	[33]	2019

were published in journals. Finally, we found 50 studies published after 2016, considering the abstract review, the technical content's development, and the conclusions while fulfilling the proposed inclusion criteria.

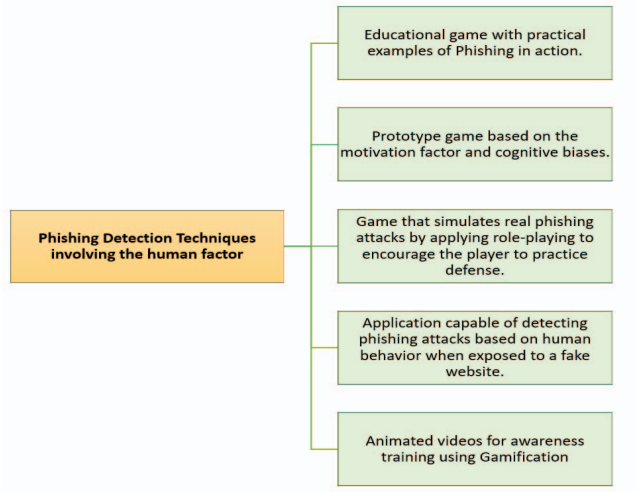

Fig. 2. Techniques involving the human factor in phishing detection

IV. EVALUATION OF RESULTS AND DISCUSSION

Concerning RQ 1, i.e., What are the human factor's techniques in phishing detection? Dixon et al. [35] mention that educational games and simulations are versatile and powerful teaching tools that can test and train players through practical examples of phishing tactics. In the same context, Kiebling et al. [36] implemented a prototype based on a game called SaltPepper, leveraging an interdisciplinary approach to improve the impact factors on information security behavior (ISB) according to the motivation factor and cognitive biases. According to Fogg's behavioral model (FBM), [36], human behavior is a product of three factors: motivation, ability, and triggers. Srinivasa Roa and Pais [23] developed an application called FeedPhish that can detect phishing attacks based on human behavior when exposed to a fake website. If the user logs in correctly, it is classified as phishing; otherwise, it is subjected to additional heuristic filtering. Younis and Musbah [6] propose a framework with two main components embedded in challenge-based games: animation videos for awareness training and a gamification part that will put users in a real test to detect actual and fake phishing attacks. Gamification is used as an evaluation method that reinforces the achieved knowledge [6]. To sum up, an explanatory chart (Figure 2) showcases the techniques and tools found in the related literature.

Concerning **RQ 2**, i.e., What are the new Cognitive Security techniques and tools in Phishing? Salahdine and Kaabouch [37] report that artificial intelligence-based defense mechanisms are the most effective techniques to reduce the risk of social engineering attacks. Cognitive computing can also reduce the shortcomings or concerns faced during big data analysis. Gupta et al. [38] conclude that the characteristics of cognitive computing (namely, observation, interpretation, evaluation, and decision) can be mapped to the five vs. of big data (i.e., volume, variety, veracity, velocity, and value). In [39], authors propose cognitive security applications using big data, machine learning, and data analytics to improve the response times in attack detection. This work analyzes anomalous behavior related to phishing web attacks and explores how machine-learning techniques can be an option to address this problem. Cho et al. [3] propose a probability model using stochastic Petri nets to examine the effect of a human individual's personality traits on trust, perceived risk, and decision performance. The results show that agreeableness and neuroticism significantly affect trust, perceived risk, and decision performance. Andrade and Yoo [13] present a cognitive security model that integrates technological solutions such as Big Data, Machine Learning, and Support Decision Systems with the cognitive processes that security analysts use to generate knowledge, understanding, and execution of security response actions. They report that cognitive security considers four components: processes, knowledge, technology, and cognitive skills. Similarly, in [34], it is argued that cognitive security could improve security analysts' cognitive skills by using technological solutions such as big data, machine learning, and data mining to generate states of cybersecurity awareness. Finally, Silva and M. Hernandez-Alvarez [40] constructed a ransomware detection and prevention model. Figure 3 summarizes the techniques used for cognitive security encountered in this SLR process.

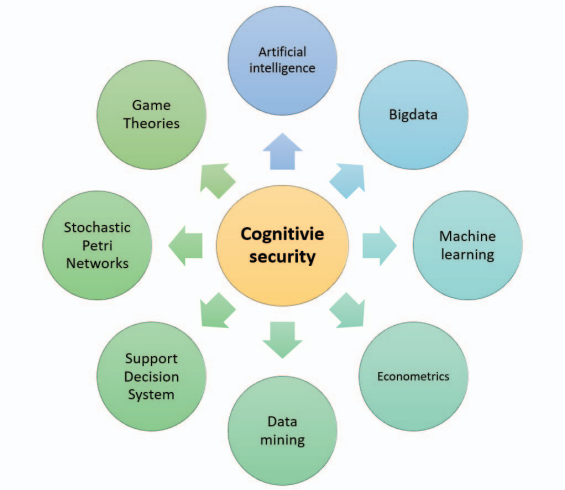

Fig. 3. Cognitive safety techniques encountered in the SLR process.

Concerning **RQ 3**, i.e., How can Cognitive Psychology be applied to phishing? In [41], the authors argue for the potential of NeuroIS (cognitive neuroscience applied to information systems) to shed new light on users' reception of security messages in the areas of (1) habituation, (2) stress, (3) fear, and (4) dual-task interference. Likewise, in [27], the authors present a proof-of-concept computer model to simulate human behavior concerning phishing website detection based on the ACT-R cognitive architecture (e.g., perception and attention, knowledge and memory, problem-solving and decision-making, as well as motor confirmation of decision). The article [42] reviews the cognitive challenges associated with the task of a CCTV operator: visual search and cognitive/perceptual overload, attention failures, vulnerability to distraction, and decision-making in a dynamically evolving environment. Surveillance is necessary to detect and prevent dangerous incidents (e.g., drowning, aircraft collision) or malicious acts (terrorism, cyber-attacks, civil disobedience). The study [43] explored the effect of using cues and cognitive load when detecting phishing emails. A total of 50 undergraduate students completed: (1) a railway monitoring task and; (2) a phishing detection task. An essential utilization assessment battery (EXPERTise 2. 0) then ranked participants with higher or lower signal utilization. As expected, higher signal utilization was associated with a higher probability of detecting phishing emails. However, variation in cognitive load did not affect phishing detection, nor was there an interaction between signal utilization and cognitive load. Threat detection was identified as why people who spend cognitive effort processing phishing communication are less likely to fall for phishing threats [29]. Musuva et al. [29] further elaborated on the role of cognitive processing in detecting and reducing phishing attacks. The proposed model is based on the elaboration probability model and is empirically tested using data from 192 cases. The results indicate that threat detection has the most potent effect on reducing susceptibility to phishing. In [49], the authors present a review of existing software tools that materialize relevant cognitive models in a way that people can use without advanced knowledge of cognitive modeling. Among the many existing tools, the focus is given to CogTool, SANLab-CM, and Coagulator. The main reason is that the latter are well-maintained open-source projects with a sizable user base. The study [45] argues that a conventional approach to cyber security awareness is ineffective in influencing employees and creating sustainable behavior change. Adopting Kelman's psychological attachment theory, the authors argue that most organizations are at the compliance level of influence, where employees comply with company policy to gain rewards or avoid punishment. Likewise, Albladi and Weir [46] claim that it is necessary to understand the factors that influence user competence in threat detection if we are to create a profile of susceptible users, develop appropriate training and mentoring programs, and generally help address this problem. In their work, they propose and validate a user-centered framework based on four perspectives: socio-psychological, habitual, socio-emotional, and perceptual. This paper investigates the susceptibility to spear phishing as a

function of the Internet user's age (old or young), influence weapon, and life domain. The reported results show that older women were the most vulnerable to phishing attacks. At the same time, younger adults were more susceptible to scarcity, and older adults were more susceptible to reciprocity. On the other hand, in [31], it is mentioned that successful emails employ psychological weapons of influence and relevant life domains. Several studies have found that current technology is inadequate regarding online security. The system developed in [47] is based on the health belief model and cooperation and competition theory. The results show that perceived threat severity, perceived barriers, perceived benefits, self-efficacy, competence, and cooperation are significant factors in predicting social engineering victimization. Figure 4 summarizes the cognitive factors that influence a Phishing attack and have to be taken into account by users and security specialists.

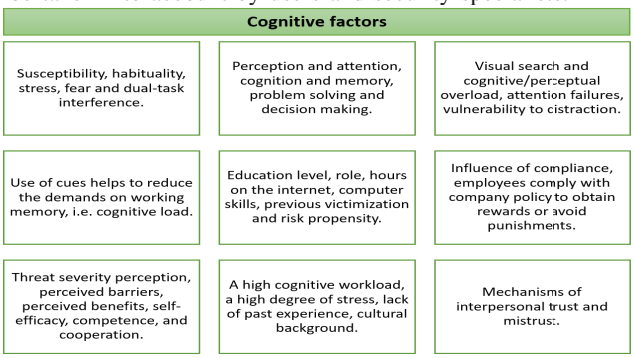

Fig. 4. Cognitive factors influencing a phishing attack

Regarding **RQ 4**, i.e., What is the human perception of risk in the face of social engineering attacks?

In [48], authors developed a questionnaire using the Qualtrics survey software to investigate people's perception of phishing email attack detection. The authors presented participants with a test of five different categories of emails (including phishing and non-phishing). The findings show that participants found detecting modern phishing email attacks challenging, even though they were alert to misspellings of older phishing email attacks. The purpose of the study [49] was to determine whether humans could distinguish fraudulent from legitimate uniform resource locators (URLs) links without the aid of specific hardware or software. To that end, the authors conducted a test with 1044 participants. The results indicate that it was difficult for participants to identify URLs when reviewing emails correctly. Alqarni et al. [50] claim that phishing is one of the most common attacks and one of the most challenging problems on social networking sites (SNSs). They describe that it is possible to predict the susceptibility of Facebook users to phishing victimization based on their demographics, anonymity, social capital, and risk perception. Wash and Cooper [22] argue that humans represent one of the most persistent vulnerabilities in many computer systems. Moreover, they compare traditional fact-and-tip training with training that uses a simple story to convey the same lessons. They found a surprising interaction effect: stories do not work as well as facts and tips, but they work much better when told by a peer or security expert. Older adults are rapidly increasing their use of online banking, social networking, and email, which carry subtle and severe security and privacy risks. Individuals with mild cognitive impairment (MCI) are particularly vulnerable to these risks because MCI may reduce their ability to recognize scams such as email phishing, follow recommended password guidelines, and consider the implications of sharing personal information [51]. In [52], the authors develop a novel model to predict user vulnerability based on various perspectives of user characteristics. The proposed model includes interactions between different social network-oriented factors, such as the level of network participation, motivation to use the network, and competence to cope with threats in the network. The results of this research indicate that most of the user characteristics are factors that directly or indirectly influence user vulnerability. A simulated phishing experiment targeting 6938 faculty and staff at George Mason University is presented in [32]. The three-week phishing campaign employed three types of phishing vulnerabilities and examined demographic data, linked network/workstation monitoring audit data, and a variety of behavioral and psychological factors measured through pre- and post-campaign surveys. In [2], the authors assessed the main underlying aspects and concepts of social engineering attacks and their influence on the New Zealand banking sector. The global financial sector has been on a continuous attack platform due to its relevance to any nation's economy. Cybercriminals will never stop perpetrating attacks; instead, they will continue to develop ingenious ways to sabotage banks and their customers. Additionality, building on the cognitive psychology literature, the authors in [53] developed an automated and fully quantitative method based on machine learning and econometrics to construct a triage mechanism leveraging the cognitive characteristics of phishing emails. The emerging Cognitive Psychology of Cybersecurity is key to understanding behavior in the traditional framework of human cognition. Some of the latest findings in the literature are [54]: (i) high cognitive workload, high stress, low attentional vigilance, lack of domain knowledge and/or lack of experience make one more susceptible to socially engineered cyberattacks; (ii) awareness or gender alone does not necessarily reduce one's susceptibility to socially engineered cyberattacks; (iii) cultural background affects one's susceptibility to socially engineered cyberattacks; and (iv) the less frequent the socially engineered cyberattacks, the greater the susceptibility to these attacks. Time pressure, workload, and the use of a "faster way of working" were some of the human factors influencing participation in risky actions by employees in organizations. The lack of research on human behavior in cybersecurity and information security further aggravates the misunderstanding of human decision-making while operating an information system [60]. The research limitation about human behavior in cybersecurity and information security further aggravates the misunderstanding of human decision-making while operating

an information system [55]. People tend to replicate interpersonal trust and distrust mechanisms to gauge their trust. Such mechanisms involve cognitive processes that people rely on before making a decision to trust or distrust. In [31], a study designed to find out how people interpret phishing emails and decide whether to trust them or not was conducted on 249 participants. It was observed that certain elements that elicit trust or distrust remained unchanged regardless of the participant. To summarise, figure 5 details the human factors involved in the perception of risk in the face of phishing attacks.

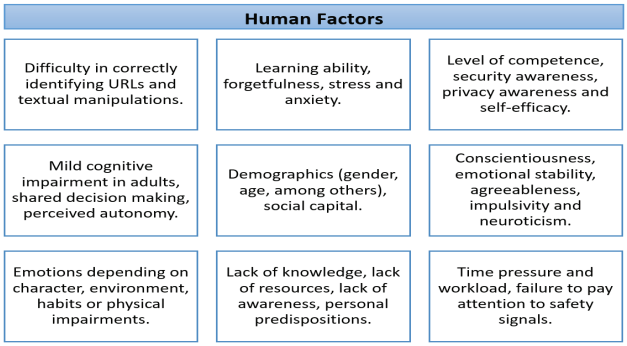

Fig. 5. Human factors influencing a phishing attack

V. Conclusions

The present systematic literature review surveys relevant studies in which human and cognitive factors are considered when performing experiments on detecting phishing attacks. One of the factors most discussed in several of the examined articles is susceptibility to phishing, as well as the factor of human behavior, trust, and distrust. Something important to mention is that stress, time pressure, fear, and lack of knowledge can influence the possibility of being victimized by attackers. Furthermore, demographic data such as age and gender are taken into consideration in some works. Another relevant research direction is cognitive security, a new topic that can help detect and mitigate phishing attacks, as demonstrated by some authors in their work. Cognitive security can be achieved through artificial intelligence, machine learning algorithms, big data methods, and mining techniques. Some researchers also highlight the importance of user training in the educational and business environment. To that end, they propose educational games that capture data on the influence of factors such as competition. Nevertheless, the training that had a better result is when it is practical training, in which actual events of phishing attacks are narrated, compared to training based on tips in a simple way. As future work, we propose implementing a prototype of training against phishing attacks in e-mails, which leverages the achievements of security and cognitive psychology to efficiently train users and, most importantly, make them aware of the responsibility they have when they open an e-mail and click without caution.

VI. Acknowledgment

The authors would like to thank the resources granted to develop the research project entitled: ”Design and Implementing the IT infrastructure and service management system for the ESPE Academic CERT”, coded as PIM-03-2020-ESPE-CERT, and to the **CERT Radical of Grupo Radical** for its technological and financial support.

References

[1] G1. B. Postnikoff y I. Goldberg, ”Robot Social Engineering: Attacking Human Factors with Non-Human Actors”, en Companion of the 2018 ACM/IEEE International Conference on Human-Robot Interaction, New York, NY, USA, mar. 2018, pp. 313-314. doi: 10.1145/3173386.3176908.

[2] D. Airehrour, N. Vasudevan Nair, y S. Madanian, Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model, Information, vol. 9, n.o 5, Art. n.o 5, may 2018, doi: 10.3390/info9050110.

[3] J.-H. Cho, H. Cam, y A. Oltramari, Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis, en 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Deci-sion Support (CogSIMA), mar. 2016, pp. 7-13. doi: 10.1109/COGSIMA.2016.7497779.

[4] G. Desolda, L. S. Ferro, A. Marrella, T. Catarci, y M. F. Costabile, Human Factors in Phishing Attacks: A Systematic Litera-ture Review, ACM Comput. Surv., vol. 54, n.o 8, p. 173:1-173:35, oct. 2021, doi: 10.1145/3469886.

[5] S. Gupta, A. Singhal, y A. Kapoor, A literature survey on social engineering attacks: Phishing attack, en 2016 International Conference on Computing, Communication and Automation (ICCCA), abr. 2016, pp. 537-540. doi: 10.1109/CCAA.2016.7813778.

[6] Y. A. Younis y M. Musbah, A Framework to Protect Against Phishing Attacks, en Proceedings of the 6th International Con-ference on Engineering MIS 2020, New York, NY, USA, sep. 2020, pp. 1-6. doi: 10.1145/3410352.3410825.

[7] Z. A. Wen, Z. Lin, R. Chen, y E. Andersen, What.Hack: Engaging Anti-Phishing Training Through a Role-playing Phishing Simulation Game, en Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, New York, NY, USA, may 2019, pp. 1-12. doi: 10.1145/3290605.3300338.

[8] Apwg, apwg_trends_report_q1_2022.pdf, [Online], Available at.:https://docs.apwg.org/reports/apwg_trends_report_q1_2022.pdf (Accessed July 1, 2022).

[9] Tripwire, Q1 2022 Phishing Threat Trends and Intelligence Report, The State of Security, June 21, 2022. https://www.tripwire.com/state-of-security/security-data-protection/phishing-threat-trends-intelligence-report/ (accessed July 1, 2022).

[10] C. A. Tian y M. L. Jensen, Effects of emotional appeals on phishing susceptibility, p. 16.

[11] J. Jeong, J. Mihelcic, G. Oliver, y C. Rudolph, Towards an Improved Understanding of Human Factors in Cybersecurity, en 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), dic. 2019, pp. 338-345. doi: 10.1109/CIC48465.2019.00047.

[12] B. Wilson, Introducing cyber security by designing mock social engineering attacks, J. Comput. Sci. Coll., vol. 34, n.o 1, pp. 235-241, oct. 2018.

[13] R. O. Andrade y S. G. Yoo, Cognitive security: A comprehensive study of cognitive science in cybersecurity, J. Inf. Secur. Appl., vol. 48, p. 102352, oct. 2019, doi: 10.1016/j.jisa.2019.06.008.

[14] M. J. Page et al., The PRISMA 2020 statement: an updated guideline for reporting systematic reviews, BMJ, p. n71, mar. 2021, doi: 10.1136/bmj.n71.

[15] R. Andrade y J. Torres, Self-Awareness as an enabler of Cognitive Security, en 2018 IEEE 9th Annual Information Technol-ogy, Electronics and Mobile Communication Conference (IEMCON), nov. 2018, pp. 701-708. doi: 10.1109/IEMCON.2018.8614798.

[16] What is Cognitive Security? https://www.cogsec.org/what-is-cognitive-security (accessed July 4, 2022).

[17] Y. Zheng, A. Moini, W. Lou, Y. T. Hou, y Y. Kawamoto, Cognitive security: securing the burgeoning landscape of mobile networks, IEEE Netw., vol. 30, n.o 4, pp. 66-71, jul. 2016, doi: 10.1109/MNET.2016.7513866.

[18] E. Roy, Cognitive Factors, en Encyclopedia of Behavioral Medicine, M. D. Gellman y J. R. Turner, Eds. New York, NY: Springer, 2013, pp. 447-448. doi: 10.1007/978-1-4419-1005-9_1116.

[19] RisklQ, RiskIQ's 2021 Evil Internet Minute — RiskIQ, July 8, 2021. https://www.riskiq.com/resources/infographic/evil-internet-minute-2021/ (accessed July 1, 2022).

[20] S. Salloum, T. Gaber, S. Vadera, y K. Shaalan, Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey, Procedia Comput. Sci., vol. 189, pp. 19-28, ene. 2021, doi: 10.1016/j.procs.2021.05.077.

[21] Z. M. Hakim et al., The Phishing Email Suspicion Test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection, Behav. Res. Methods, vol. 53, n.o 3, pp. 1342-1352, jun. 2021, doi: 10.3758/s13428-020-01495-0.

[22] R. Wash y M. M. Cooper, Who Provides Phishing Training? Facts, Stories, and People Like Me, en Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, New York, NY, USA, abr. 2018, pp. 1-12. doi: 10.1145/3173574.3174066.

[23] R. Srinivasa Rao y A. R. Pais, Detecting Phishing Websites using Automation of Human Behavior, en Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security, New York, NY, USA, abr. 2017, pp. 33-42. doi: 10.1145/3055186.3055188.

[24] S. Chaudhary, E. Berki, L. Li, J. Valtanen, y M. Helenius, A Socio-Cognitive and Computational Model for Decision Making and User Modelling in Social Phishing, p. 15.

[25] P. Tiwari, EXPLORING PHISHING SUSCEPTIBILITY ATTRIBUTABLE TO AUTHORITY, URGENCY, RISK PERCEPTION AND HUMAN FACTORS, thesis, Purdue University Graduate School, 2020. doi: 10.25394/PGS.12739592.v1.

[26] C. I. Canfield, B. Fischhoff, y A. Davis, Quantifying Phishing Susceptibility for Detection and Behavior Decisions, Hum. Factors, vol. 58, n.o 8, pp. 1158-1172, dic. 2016, doi: 10.1177/0018720816665025.

[27] N. Williams y S. Li, Simulating Human Detection of Phishing Websites: An Investigation into the Applicability of the ACT-R Cognitive Behaviour Architecture Model, en 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), jun. 2017, pp. 1-8. doi: 10.1109/CYBConf.2017.7985810.

[28] A. Vishwanath, B. Harrison, y Y. J. Ng, Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility, Commun. Res., vol. 45, n.o 8, pp. 1146-1166, dic. 2018, doi: 10.1177/0093650215627483.

[29] P. M. W. Musuva, K. W. Getao, y C. K. Chepken, A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility, Comput. Hum. Behav., vol. 94, pp. 154-175, may 2019, doi: 10.1016/j.chb.2018.12.036.

[30] P.-E. Arduin, A cognitive approach to the decision to trust or distrust phishing emails, Int. Trans. Oper. Res., vol. n/a, n.o n/a, doi: 10.1111/itor.12963.

[31] D. Oliveira et al., Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing, en Proceedings of the 2017 CHI Conference on Human Factors in Com-puting Systems, New York, NY, USA, may 2017, pp. 6412-6424. doi: 10.1145/3025453.3025831.

[32] F. L. Greitzer, W. Li, K. B. Laskey, J. Lee, y J. Purl, Experimental Investigation of Technical and Human Factors Related to Phishing Susceptibility, ACM Trans. Soc. Comput., vol. 4, n.o 2, p. 8:1-8:48, jun. 2021, doi: 10.1145/3461672.

[33] E. A. Cranford, P. Rajivan, y P. Aggarwal, Modeling Cognitive Dynamics in End-User Response to Phishing Emails, p. 6.

[34] R. Andrade, J. Torres, y S. Cadena, Cognitive Security for Incident Management Process, en Information Technology and Systems, Cham, 2019, pp. 612-621. doi: 10.1007/978-3-030-11890-7_59.

[35] M. Dixon, N. A. Gamagedara Arachchilage, y J. Nicholson, Engaging Users with Educational Games: The Case of Phish-ing, en Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems, New York, NY, USA, may 2019, pp. 1-6. doi: 10.1145/3290607.3313026.

[36] S. Kießling, T. Hanka, y D. Merli, Saltamp;Pepper: Spice up Security Behavior with Cognitive Triggers, in European In-terdisciplinary Cybersecurity Conference, New York, NY, USA: Association for Computing Machinery, 2021, pp. 26-31. Ac-cessed May 25, 2022. [Online]. Available at: https://doi.org/10.1145/3487405.3487656.

[37] F. Salahdine y N. Kaabouch, Social Engineering Attacks: A Survey, Future Internet, vol. 11, n.o 4, Art. n.o 4, abr. 2019, doi: 10.3390/fi11040089.

[38] S. Gupta, A. K. Kar, A. Baabdullah, y W. A. A. Al-Khowaiter, Big data with cognitive computing: A review for the future, Int. J. Inf. Manag., vol. 42, pp. 78-89, oct. 2018, doi: 10.1016/j.ijinfomgt.2018.06.005.

[39] I. Ortiz Garcés, M. F. Cazares, y R. O. Andrade, Detection of Phishing Attacks with Machine Learning Techniques in Cogni-tive Security Architecture, en 2019 International Conference on Computational Science and Computational Intelligence (CSCI), dic. 2019, pp. 366-370. doi: 10.1109/CSCI49370.2019.00071.

[40] J. A. Herrera Silva y M. Hernández-Alvarez, Large scale ransomware detection by cognitive security, en 2017 IEEE Sec-ond Ecuador Technical Chapters Meeting (ETCM), oct. 2017, pp. 1-4. doi: 10.1109/ETCM.2017.8247484.

[41] B. Brinton Anderson, A. Vance, C. B. Kirwan, D. Eargle, y J. L. Jenkins, How users perceive and respond to security messag-es: a NeuroIS research agenda and empirical study, Eur. J. Inf. Syst., vol. 25, n.o 4, pp. 364-390, jul. 2016, doi: 10.1057/ejis.2015.21.

[42] H. M. Hodgetts, F. Vachon, C. Chamberland, y S. Tremblay, See No Evil: Cognitive Challenges of Security Surveillance and Monitoring, J. Appl. Res. Mem. Cogn., vol. 6, n.o 3, pp. 230-243, sep. 2017, doi: 10.1016/j.jarmac.2017.05.001.

[43] G. Nasser, B. W. Morrison, P. Bayl-Smith, R. Taib, M. Gayed, y M. W. Wiggins, The Effects of Cue Utilization and Cognitive Load in the Detection of Phishing Emails, en Financial Cryptography and Data Security, Cham, 2020, pp. 47-55. doi: 10.1007/978-3-030-54455-3_4.

[44] H. Yuan, S. Li, y P. Rusconi, Review of Cognitive Modeling Software Tools, en Cognitive Modeling for Automated Human Performance Evaluation at Scale, H. Yuan, S. Li, y P. Rusconi, Eds. Cham: Springer International Publishing, 2020, pp. 17-26. doi: 10.1007/978-3-030-45704-4_3.

[45] M. Alshaikh y B. Adamson, From awareness to influence: toward a model for improving employees' security behaviour, Pers. Ubiquitous Comput., vol. 25, n.o 5, pp. 829-841, oct. 2021, doi: 10.1007/s00779-021-01551-2.

[46] S. M. Albladi y G. R. S. Weir, User characteristics that influence judgment of social engineering attacks in social networks, Hum.-Centric Comput. Inf. Sci., vol. 8, n.o 1, p. 5, feb. 2018, doi: 10.1186/s13673-018-0128-7.

[47] A. Alturki, N. Alshwihi, y A. Algarni, Factors Influencing Players' Susceptibility to Social Engineering in Social Gaming Networks, IEEE Access, vol. 8, pp. 97383-97391, 2020, doi: 10.1109/ACCESS.2020.2995619.

[48] F. Carroll, J. A. Adejobi, y R. Montasari, How Good Are We at Detecting a Phishing Attack? Investigating the Evolving Phishing Attack Email and Why It Continues to Successfully Deceive Society, SN Comput. Sci., vol. 3, n.o 2, p. 170, feb. 2022, doi: 10.1007/s42979-022-01069-1.

[49] E. Pearson, C. L. Bethel, A. F. Jarosz, y M. E. Berman, "To click or not to click is the question": Fraudulent URL identification accuracy in a community sample, en 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), oct. 2017, pp. 659-664. doi: 10.1109/SMC.2017.8122682.

[50] Z. Alqarni, A. Algarni, y Y. Xu, Toward Predicting Susceptibility to Phishing Victimization on Facebook, en 2016 IEEE International Conference on Services Computing (SCC), jun. 2016, pp. 419-426. doi: 10.1109/SCC.2016.61.

[51] H. M. Mentis, G. Madjaroff, y A. K. Massey, Upside and Downside Risk in Online Security for Older Adults with Mild Cognitive Impairment, en Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, New York, NY, USA, may 2019, pp. 1-13. doi: 10.1145/3290605.3300573.

[52] S. M. Albladi y G. R. S. Weir, Predicting individuals' vulnerability to social engineering in social networks, Cybersecurity, vol. 3, n.o 1, p. 7, mar. 2020, doi: 10.1186/s42400-020-00047-5.

[53] L. Allodi, a.v.d.heijden@student.tue.nl Eindhoven University of Technology, p. 19.

[54] Frontiers — Human Cognition Through the Lens of Social Engineering Cyberattacks — Psychology. https://www.frontiersin.org/articles/10.3389/fpsyg.2020.01755/full (accessed June 13, 2022).

[55] C. Nobles, Botching Human Factors in Cybersecurity in Business Organizations, Holistica, vol. 9, pp. 71-88, dic. 2018, doi: 10.2478/hjbpa-2018-0024.