Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 239 (2024) 526–533

Procedia Computer Science

www.elsevier.com/locate/procedia

CENTERIS – International Conference on ENTERprise Information Systems / ProjMAN – International Conference on Project MANagement / HCist – International Conference on Health and Social Care Information Systems and Technologies 2023

The use of gamification on cybersecurity awareness of healthcare professionals

Ana Carreiro [1,2,4]*, Carina Silva[1,2], Mário Antunes[3,5]

[1] Lisbon School of Health Technology, Polytechnic Institute of Lisbon, Portugal
[2] Health and Technology Research Center, Lisbon, Portugal
[3] Polytechnic of Leiria, School of Technology and Management, Leiria, Portugal
[4] Hospital do Divino Espírito Santo de Ponta Delgada, EPER, Azores, Portugal
[5] Center for Research in Advanced Computing Systems, INESC-TEC, Portugal
2012031@alunos.estesl.ipl.pt, carina.silva@estesl.ipl.pt. mario.antunes@ipleiria.pt

Abstract

Cybersecurity has a major impact on the healthcare sector, mainly due to the sensitive data and vital medical devices that, when an attack occurs, may compromise the life, safety, and well-being of the patients. However, those institutions fail on implementing correct system protection policies and providing adequate programs for cybersecurity training and raising cybersecurity awareness. Healthcare professionals develop their academic courses focusing on providing the best care for the patients, studying guidelines, treatment protocols, and diagnostic criteria. However, there are insufficient subjects dedicated to the development of digital literacy to match the requisites of the daily challenges of those professionals, with human error being the main cause of data breaches worldwide. So, developing training programs to face the cybersecurity day-to-day threats is mandatory.

Broadly speaking, traditional training programs seem to fail on retaining students' motivation, engagement, and long-term knowledge acquisition, being time-consuming and challenging in scheduling and planning. To face this situation, new techniques, such as gamification, have emerged, with promising results on motivation and engagement, allowing the users to be the center of the training programs, matching the strategy to their levels of knowledge and preferences.

This paper aims to identify the existing gamified approaches available, review the state-of-the-art related to gamification and cybersecurity training, and elaborates on how they can be successfully applied to training programs for healthcare professionals.

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
E-mail address: 2012031@alunos.estesl.ipl.pt

10.1016/j.procs.2024.06.202

Keywords: gamification: cybersecurity; healthcare; cyber awareness

1. Introduction

Nowadays, technology walks side by side with medical advances and patient prognostic improvement. It can be found everywhere inside a medical facility, leading to more accurate diagnoses of pathologies and more effective treatment. Known as the Internet of Medical Things (IoMT), the possibility to connect medical devices and applications used in healthcare to networks expands the physical barriers of health institutions to areas beyond reach [1]. This expansion has allowed the growth of telemedicine, which has been crucial in hospitals, for example during the Covid-19 pandemic period. However, these technological advances are also accompanied by new cybersecurity challenges. Safety, now, is not just a matter of keeping information physically restrained, but also a matter of keeping devices safe. Being connected to the Internet, IoMT devices are more susceptible to cybercrime, as physical barriers to prevent the penetration and stealing of information vanish and attacks can emerge from anywhere around the world.

Technology can be found in almost every process integrated into health institutions’ daily activities. Electronic health records and patient personal and clinical information is easily stored, accessed, and shared among healthcare workers in different health institutions [2]. The expansion of the technology used for almost every task also means that, if an attack occurs, the workflow of the facility will be severely compromised, incurring important damage and costs.

Healthcare institutions are appealing targets to hackers, because of the amount of sensitive data they usually hold and the general low investment in advanced cybersecurity infrastructures [3]. Most of the cyberattacks in the health sector occur due to a low level of cybersecurity awareness by the main healthcare workers, namely physicians, nurses, administrative staff, and management board, just to mention a few. Consequently, the strategies to minimize cybersecurity vulnerabilities must also recognize healthcare workers, developing methods to provide effective training on cybersecurity to these professionals.

In a sector that has limited resources and with distinctive needs from others, some questions arise: how to keep up and do better, and how to level the diversity of educational backgrounds and dull its differences? Fortunately, creative, and innovative solutions have been developed and applied to human resources training programs, namely the emergent technologies related to the gamification of training methods.

Gamification has emerged as a new tool to turn training and education more appealing and has shown positive results when applied to cybersecurity training [4]. In fact, traditional training sessions are usually time-consuming, with poor results on motivation, engagement, and knowledge retaining when compared to gamified strategies. It is possible to find some commercialized solutions designed for this purpose, but none is specific to the healthcare business and its workers.

This paper describes the state-of-the-art on using gamification strategy in cybersecurity training, emphasizing it as ab adequate strategy to implement in the health sector. The paper is organized as follows: in Section 2, the main concepts related to cybersecurity and its implication on health are explored. Section 3 is dedicated to gamification as well as its application in cybersecurity training. Next in Section 4, the application of a gamified training program on cybersecurity to the health sector is discussed. Finally, Section 5 presents the conclusions and delineates some future directions for this research.

2. Cybersecurity in health

According to ISO/IEC 27032:2012, cybersecurity is the «preservation of confidentiality, integrity and availability of information in cyberspace» [5]. By its turn, cyberspace can be defined as the «complex environment resulting from the interaction of people, software, and services on the Internet using technology devices and networks connected to it, which does not exist in any physical form» [5].

Safe cyberspace can only be achieved by the combination of multidisciplinary techniques, focused on attitudes, behaviors, knowledge, and awareness of the organization's personnel about common cyber risks and threats, creating a new concept of cybersecurity culture. This culture involves education programs, IT infrastructure auditing, and the review of security policies to make hospital personnel more aware when processing sensitive information in daily business operations, thus preventing attacks or leakages [6].

It Is undeniable that technology has been a major factor in the improvement of the healthcare sector, facilitating access to real-time information, clinical interventions, and diagnoses. However, it also comes along with new challenges regarding privacy and safety matters. Healthcare institutions represented 27% of the targets of cyberattacks in Europe, in 2018 [6]. In Portugal, the reality is similar. In 2021, divided by several domains of activity, Portuguese institutions were attacked 881 times per week, representing an increase of 81% when compared to 2020. The most represented areas were Education, Health, and Public Administration [7].

Besides the impact cyberattacks have on institutions' public image and reputation, the economic costs are also very accountable. In 2017, WannaCry, a ransomware attack that affected United Kingdom's National Health System, had an estimated cost of 105 million Euros, and more than 19 thousand appointments were canceled, representing a major impact on the normal function of the health system [8]. This ransomware attack also affected many businesses worldwide and was originated by the download of an infected (malware) file, that encrypted the files of a computer and demanded a ransom to unlock them [9]. Ransomware is often associated with phishing and can be prevented if the user is able to recognize it as a threat, not downloading or clicking on any link that may be associated with the fake e-mail message. Therefore, this attack could be prevented if the users were aware of this cyberattack technique and able to recognize it.

Phishing, ransomware, loss/theft of equipment or data, insider, accidental, or intentional data loss, and attacks against connected medical devices are the most common mechanisms that compromise data safety in Hospitals [2], as summarized in Table 1. Most of these techniques target humans and the probability of successful attacks is seriously diminished if the user is capable to recognize them as threats and adopting correct attitudes. But this is only possible if institutions guarantee their professionals have a good level of cybersecurity awareness, providing regular training and education.

Table 1. Most common cyberattack threats affecting the health sector (adapted from Ahmed et. al. 2022).

Cyberattack Type	Definition
E-mail Phishing	Attempt to steal information by sending a suspicious link via e-mail that seems legit and redirects to a website to access sensitive information or infect the system.
Ransomware	It is malware that infects the computer or the network and steals the data, encrypting them, and requiring a ransom to retrieve access to the data. This can be a result of e-mail phishing.
Loss/Theft of Equipment or Data	Devices such as laptops, tablets, and phones used in hospitals may contain sensitive and clinical data that, if stolen or lost, may lead to unauthorized access and dissemination of the information, compromising patient safety.
Insider accidental or Intentional Data Loss	Insider accidental data loss relates to mistakes resulting without the intention to harm or benefit from it. Intentional data loss results from the use of the technology or network to benefit personally, due to negligence in sharing and storing data, lack of access limitation to sensitive data, and lack of awareness.
Attacks against connected medical devices	Those attacks may significantly harm the patient, compromising their survival, and resulting in unauthorized access to its configuration, changing it and leading to inaccurate measures or treatments.

So, considering that the major types of cyberattacks and their techniques target users, stakeholders must consider the level of cybersecurity awareness of their workers with the same importance as the acquisition of the newest cybersecurity protecting systems and technology.

Guaranteeing the human factor can recognize threats and minimize their potentially negative effects is vital to ensure data safety and a safe application of technology development on health. Unfortunately, regarding the work from Nunes et. al., Portuguese health professionals have low levels of cybersecurity awareness, putting Portuguese health institutions at a high risk of cyberattacks [10]. Consequently, security issues cannot be addressed using only technical specifications [11].

Human error is associated with more than 80% of cyber incidents and malware attacks [12]. Providing proper training for workers is mandatory to raise cybersecurity awareness and mitigate the effects of successful attacks, aligned with the recommendations defined by the work of Ahmed et al. (2022). This work aimed to review the state-of-the-art related to cybersecurity in healthcare, which concluded that regular training of professionals (at least one session a year) significantly decreased the impact of cyberattacks [2].

3. Gamification

The term "gamification" was first coined in 2002 but it only became popular around 2010 [13]. It can be defined as the use of elements typically found in game design applied to nongame-related businesses and applications. Gamification has reached many domains, such as health and well-being, sports, social networks, sustainability, e-commerce, productivity, learning, and education. When talking about organizations and enterprises, gamification can be found in processes like human resources management (recruitment, onboarding, developing programs, and training), marketing, and customer support. The 2019 Gamification at Work survey, elaborated by TalentLMS, stated that companies that apply gamification strategies reach an 89% increment in their productivity, and an 88% increment in employee satisfaction when compared to the ones that do not recur to gamification [14].

Specifically, when talking about education and training programs for employees, about 90% of the competencies gained with traditional training programs are forgotten over a year. Traditional training sessions have several limitations described in the literature and summarized in the following: the program's dynamics fail to retain attenders' attention, have a stricter structure, and do not match the expectations and the culture of different generations, such as the millennials and generation Z, born in the digital era [15].

Gamification is a powerful tool that overcomes the limitations of traditional training programs and allows the user to have a more gratifying experience, increasing motivation and engagement [14]. A study developed by the Massachusetts Institute of Technology (MIT) concluded that gamification training sessions led to a 90% increment in the retaining of learned content and the number of training sessions concluded had tripled. In fact, motivation activates some structural zones of the brain, such as the limbic system and the hippocampus, which are involved in the process of acquiring information, consolidating, and storing, therefore improving learning processes [15].

Finally, gamification also allows a process to be a "Human-Focused Design", considering other aspects than pure efficiencies, such as human motivation to use it [16]. However, the success of a gamified training program depends mostly on its adequacy to the users' profile.

3.1. Gamification applied to cybersecurity training and awareness

Human error is the main cause of data breaches worldwide, so it is very important to raise awareness about cybersecurity and its implications for the organization and the employees [17]. Companies should invest in gamification strategies to raise cybersecurity awareness for several reasons. It has been proven that gamification is a good solution to cybersecurity training since it challenges the players and increases their motivation due to the use of rewarding systems, audio, and video elements [15] while promoting active learning and increasing retention of the learned skills in comparison to traditional learning approaches [18].

It is possible to find several commercial gamified strategies and applications designed to provide cybersecurity training for professionals from IT, finance, engineering, and other areas, as detailed in Table 2.

Table 2. Gamified solutions for cybersecurity training.

Game name	Cybersecurity topics	Platform	Reference
What.Hack	Phishing emails	Computer game	[22]
Elevation of privileges (EOP)	Spoofing Tampering Repudiation Information Disclosure Denial of service Elevation of privileges	Card game	https://agilestationery.com/products/elevation-of-privilege-game
Cyber CIEGE	Cybersecurity definitions, Information value, Access control, Social engineering, Malware, Data protection, Physical security	Computer game	https://nps.edu/web/c3o/cc_intro
DG Data Defender	Data loss prevention	Computer game	https://digitalguardian.com/blog/gamification-data-loss-prevention-educating-and-enabling-employees-dlp
PWC Game of Treats	Cyber Threat Simulation, Responses to cyber attacks, Prevention of cyber attacks, Understanding how the attacks work, Cybersecurity awareness	Computer game	https://www.pwc.com/lk/en/assets/CS/Got-linkdin-v1.0.pdf https://www.pwc.com/lk/en/services/consulting/cybersecurity/game-of-threats.html
CyberAWARE	Phishing simulations Awareness training Cyber security toolkit	Desktop and mobile app	[26]
CounterMeasures	Basic knowledge	Desktop app	[23]
CyberNEXS	System assessment Penetration prevention	Desktop app	[24]
CyberProtect	Basic knowledge	Desktop app	[25]
Defend the Crown	Basic knowledge of technology and cyberattacks Most common techniques	Mobile app	https://www.cisa.gov/cybergames

Although there are several gamified solutions currently available and applied to cybersecurity training, most of them are paid and targeted to specific sectors such as finance or engineering. Moreover, the free-to-use ones are very simple, as they target children and the general audience, focus on general cyber awareness, and lack trying to explore specifically the healthcare sector cybersecurity challenges.

The solutions presented in Table 2 are mostly dedicated to cybersecurity awareness, however basic technical knowledge and cyberattack techniques are also very common subjects. The presentation of the solutions varies from simple card games to more complex computer games.

“CyberCIEGE” was created by US Naval School, and “Defend the Crown” was also created by US government entities, so gamification applied to cybersecurity training and awareness is being explored and valorized by important international entities in the field of cybersecurity, a significant finding that supports the use of gamification for this purpose. Nevertheless, it was not possible to find a solution specifically designed for the health sector, addressing healthcare workers’ profile of knowledge, their daily challenges, and their reality, which are different from the profile of competencies of employees from other domains.

4. Discussion

Cybersecurity has a major impact on the health sector. The major threats that compromise the health sector target the main operators and users of technology: the employees. So, to fight cybercrime, it is important to consider all the stakeholders, besides investing in IT infrastructure, promoting health employees' awareness, and motivating them to act as proactive defenders of patient data [19], where education and training play a central role. By paying attention to their attitudes and actions, and being able to recognize and mitigate the threats, health professionals will be able to fight cybercrime and improve health organizations' level of security.

Healthcare workers are trained to provide care for the patients. During their academic course, there are no specific subjects that address cybersecurity and other information technology fundamental skills. Additionally, healthcare workers have singular backgrounds, different academic programs, and tasks, according to their profession, that represent different needs and proficiency levels related to technology's usage.

Health sector workers make a heterogeneous population where "one-size fits all" strategies will eventually fail. Offering effective training is required and fundamental to mitigate the low level of cybersecurity awareness shown by the health professionals. But it is also crucial to consider a strategy that can combine efficient time and resources management, with good results on knowledge acquisition and retaining. And when looking at all this together, gamification may be the answer.

The use of a gamified strategy allows us to better manage resources and time, crucial in a sector that is heavily affected by low resources and variable demand when every second counts. Gamified training programs can be managed by the player itself, according to his rhythm and availability. Moreover, it allows for improved knowledge retention, adherence, and motivation, resulting in a long-time impact on the education program, and empowering healthcare professionals.

The use of cybersecurity gamified training solutions is applied to diverse fields of business, with proven positive results on cyber awareness. Even though there was not possible to find a solution available designed for the health sector, the primary work of DeCarlo et. al. [20] allowed us to conclude that the adoption of a gamified training strategy to provide cybersecurity training has positive results on cyber awareness of healthcare workers as well. DeCarlo et. al applied a gamified training session on cybersecurity to a sample of healthcare workers and accomplished that the levels of cybersecurity awareness improved, as well as the number of reported incidents to IT when compared to traditional training [20]. Considering the impact that cyberattacks have on the functioning of healthcare organizations, reducing their probability of success by training the professionals is vital and it is the only way to lessen the human factor in cybersecurity.

Being widely used in other sectors, including as a validated method of official initiatives to promote cybersecurity and cyber awareness deployed by governmental entities, the authors believe that the development of a gamified solution to provide education and training to healthcare professionals would be a very powerful tool to overcome the low level of cybersecurity awareness among those professionals. The adoption of a gamified solution becomes more urgent in a sector that struggles with resource and time management, allowing it to deploy a complete training program without having to allocate human and physical resources to it.

The effectiveness of the developed solution depends on how it is created according to national references on cybersecurity, aligning the cybersecurity topics with the proficiency levels required for the sector and for those professionals. It is important to consider that healthcare workers have distinct profiles from professionals dedicated to IT or finance, for instance.

In Portugal's context, it is relevant to align the cybersecurity topics to be included in the training sessions with the recommendations of the National Center of Cybersecurity (*Centro Nacional de Cibersegurança, CNCS).* The authors believe that the roadmap developed by *CNCS*, entitled *Referencial de Competências e Conhecimentos* (`https://www.cncs.gov.pt/pt/referencial-de-competencias/`) is a must use reference for this purpose. *CNCS* is a government agency that is responsible for protecting Portugal's critical infrastructure and digital assets from cyber threats, being responsible for promoting cybersecurity awareness among citizens, and businesses. The roadmap *Referencial de Competências e Conhecimentos* is a document organized by different domains and sub-domains related to cybersecurity, dividing them into numerous competencies and knowledge topics, and this document was constructed to help to define the minimum cyber awareness competencies for different businesses.

5. Conclusions and future work

This paper explores the use of gamified cybersecurity training programs for health professionals as a new way to address the low levels of cybersecurity awareness among healthcare workers. In a sector so fustigated by cybercrime, the adoption of measures and procedures to mitigate its chances and adverse impacts are fundamental, especially the ones addressing human factor as a central concern for the problem.

The application of gamified training programs on cybersecurity has been largely used in other sectors with a positive impact, but it was not possible to find a solution designed for healthcare, nor the regular use of this approach to provide cybersecurity training for health professionals, which have a profile and daily challenges so different from areas such as finance, engineering, or IT, for instance.

The combination of the good results driven by the implementation of cybersecurity gamified training programs in other sectors as well as the urgent need to improve cyber resilience and cyber awareness among health workers, motivated the authors to develop a gamified strategy to provide cybersecurity training. A multidisciplinary team, consisting of healthcare workers and cybersecurity experts, will develop a strategy that considers the profiles and daily needs of health professionals. This deployed methodology and framework are currently under development and will be soon ready to be tested in a Portuguese Hospital. The results of the implementation of the strategy will allow us to perceive the impact of a gamified cybersecurity training program on the cybersecurity awareness levels of health professionals, along with its capability to improve the cyber resilience of health institutions.

Gamification may become a solution to enhance training and mitigate the cyber risk of health institutions, improving cybersecurity awareness and enabling health professionals to become proactive safeguards of the data and devices.

Acknowledgements

This work is partially financed by national funds through *Concurso Interno de Projetos de Investigação, Desenvolvimento, Inovação e Criação Artística* (ID&CA) from Polytechnical Institute of Lisbon under the project IPL/2022/HeCyGame_ESTeSL.

References

[1] What is IoMT (Internet of Medical Things) or healthcare IoT? | Definition from TechTarget n.d. https://www.techtarget.com/iotagenda/definition/IoMT-Internet-of-Medical-Things (accessed June 2023).

[2] Ahmed MA, Sindi HF, Nour M. Cybersecurity in Hospitals: An Evaluation Model. Journal of Cybersecurity and Privacy 2022;2:853–61. https://doi.org/10.3390/jcp2040043.

[3] Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, et al. Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors 2021;21:1–25. https://doi.org/10.3390/s21155119.

[4] Onduto B, Doctoral P, Ali R, Smed AJ. Gamification of Cyber Security Awareness – A Systematic Review of Games. Computing, Faculty of Technology 2021.

[5] ISO. ISO/IEC 27032:2012. n.d.

[6] Gioulekas F, Stamatiadis E, Tzikas A, Gounaris K, Georgiadou A, Michalitsi-psarrou A, et al. A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. Healthcare (Switzerland) 2022;10:1–19. https://doi.org/10.3390/healthcare10020327.

[7] Ciberataques a organizações portuguesas aumentaram 81% em 2021 n.d. https://www.itsecurity.pt/news/news/ciberataques-a-organizacoes-portuguesas-aumentaram-81-em-2021 (accessed June 2023).

[8] WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled | UK Healthcare News n.d. https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled (accessed June 2023).

[9] Collier R. NHS ransomware attack spreads worldwide. CMAJ: Canadian Medical Association Journal 2017;189:E786. https://doi.org/10.1503/CMAJ.1095434.

[10] Nunes P, Antunes M, Silva C. Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions. Procedia Comput Sci 2021;181:173–81. https://doi.org/10.1016/j.procs.2021.01.118.

[11] Yeng PK, Fauzi MA, Yang B. A Comprehensive Assessment of Human Factors in Cyber Security Compliance Toward Enhancing the Security Practice of Healthcare Staff in Paperless Hospitals. Information (Switzerland) 2022;13. https://doi.org/10.3390/info13070335.

[12] Triplett WJ. Addressing Human Factors in Cybersecurity Leadership. Journal of Cybersecurity and Privacy 2022;2:573–86. https://doi.org/10.3390/jcp2030029.

[13] Xu Y, Chen Z, Peng MYP, Anser MK. Enhancing Consumer Online Purchase Intention Through Gamification in China: Perspective of Cognitive Evaluation Theory. Front Psychol 2020;11:1–13. https://doi.org/10.3389/fpsyg.2020.581200.

[14] Queirós R, Pinto M. Gamificação aplicada às organizações e ao ensino. ISBN: 978-972-722-922-2; PACTOR. Lidel; 2022.

[15] Villegas E, Fonseca D, Peña E, Bonet P, Fernández-guinea S. Qualitative assessment of effective gamification design processes using motivators to identify game mechanics. Sensors 2021;21:1–20. https://doi.org/10.3390/s21072556.

[16] Chou Y-K. Yu-kai Chou: Gamification & Behavioral Desing. The Octalysis Framework for Gamification & Behavioral Design n.d. https://yukaichou.com/gamification-examples/octalysis-complete-gamification-framework/ (accessed June 2023).

[17] Moore M. Bringing Gamification to Cyber Security Awareness Training. University of San Diego n.d. https://onlinedegrees.sandiego.edu/bringing-gamification-to-cyber-security-training/ (accessed June 2022).

[18] Adams M, Makramalla M. Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. Technology Innovation Management Review 2015;5:5–14. https://doi.org/10.22215/timreview/861.

[19] The importance of cybersecurity in protecting patient safety | Cybersecurity | Center | AHA n.d. https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety (accessed June, 2023).

[20] Sean D. Running head: GAMIFICATION OF CYBERSECURITY TRAINING IN HEALTHCARE Measuring the Application of Knowledge Gained from the Gamification of Cybersecurity Training in Healthcare by Sean M. DeCarlo Master of Science, Robert Morris University, 2017 Bachelo 2020.

[21] Centro Nacional de Cibersegurança. Referencial de Competências em Cibersegurança. https://www.cncs.gov.pt/pt/referencial-de-competencias/ (accessed June 2023).

[22] Wen ZA, Lin Z, Chen R, Andersen E. What.Hack: Engaging Anti-Phishing Training through a Role-playing Phishing Simulation Game. Conf Hum Factors Comput Syst - Proc. 2019;1–12

[23] Jordan, C., Knapp, M., Mitchell, D., Claypool, M., & Fisler, K. 2011. CounterMeasures: A Game for Teaching Computer Security. In Proceedings of the 10th Annual Workshop on Network and Systems Support for Games: Article 7. Piscataway, NJ: IEEE Press

[24] Nagajaran et al 2012 Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. 2012. Exploring Game Design for Cybersecurity Training. In Proceedings of the 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER): 256–262. May 27–31, 2012, Bangkok, Thailand. http://dx.doi.org/10.1109/CYBER.2012.6392562

[25] Labuschagne, W. A., Veerasamy, N., Burke, I., & Eloff, M. M. 2011. Design of Cyber Security Awareness Game Utilizing a social media Gramework. In Information Security South Africa, 1–9. Johannesburg, SA: IEEE. http://dx.doi.org/10.1109/ISSA.2011.6027538

[26] Giannakas F, Kambourakis G, Gritzalis S. CyberAware: A mobile game-based app for cybersecurity education, and awareness. Proc 2015 Int Conf Interact Mob Commun Technol Learn IMCL 2015. 2015;(May 2016):54–8.