

INSTITUTO POLITÉCNICO DE LISBOA
ESCOLA SUPERIOR DE TECNOLOGIA DA SAÚDE
DE LISBOA

UNIVERSIDADE DO ALGARVE
ESCOLA SUPERIOR DE SAÚDE

**GAMIFICAÇÃO APLICADA À FORMAÇÃO EM
CIBERSEGURANÇA DE PROFISSIONAIS DE
SAÚDE - UMA PROVA DE CONCEITO**

Ana Teresa Costa Aguiar Carreiro

Professora Doutora Carina Soares da Silva

Instituto Politécnico de Lisboa

Escola Superior de Tecnologia da Saúde de Lisboa (ESTeSL)

Professor Doutor Mário João Gonçalves Antunes

Instituto Politécnico de Leiria

Escola Superior de Tecnologia e Gestão (ESTG)

Mestrado em Gestão e Avaliação de Tecnologias em Saúde

Lisboa, 2023

INSTITUTO POLITÉCNICO DE LISBOA
ESCOLA SUPERIOR DE TECNOLOGIA DA SAÚDE DE
LISBOA
UNIVERSIDADE DO ALGARVE
ESCOLA SUPERIOR DE SAÚDE

**GAMIFICAÇÃO APLICADA À FORMAÇÃO EM
CIBERSEGURANÇA DE PROFISSIONAIS DE
SAÚDE - UMA PROVA DE CONCEITO**

Ana Teresa Costa Aguiar Carreiro

Orientadora

Professora Doutora Carina Soares da Silva

Instituto Politécnico de Lisboa (IPL)

Escola Superior de Tecnologia da Saúde de Lisboa (ESTeSL)

Orientador

Professor Doutor Mário João Gonçalves Antunes

Instituto Politécnico de Leiria

Escola Superior de Tecnologia e Gestão (ESTG)

Júri

Arguente: Professor Doutor Ricardo Queirós (Escola Superior de Media,
Artes e Design do Instituto Politécnico do Porto)

Presidente: Professora Doutora Margarida Eiras (ESTeSL, IPL)

Mestrado em Gestão e Avaliação de Tecnologias em Saúde

Lisboa, 2023

“We cannot solve problems with the kind of thinking we employed when we came up with them.”

- Albert Einstein

Acknowledgements

This project represents an innovative and totally different challenge for me. Being graduated in health sciences, cybersecurity and gamification was a completely new world. This project was only possible with the support and help from my supervisors, family, and friends. Therefore, I want to thank:

To my supervisor, Prof. Carina Silva, PhD, for being so supportive and committed to this project, allowing for new experiences to take place.

To my supervisor, Prof. Mário Antunes, PhD, for believing in me, motivating me to always do better, challenging me away from my comfort zone.

Thank you, Prof. Carina, and Prof. Mário, for your constant availability, for the encouragement and, most importantly, for your dedication to this project! All the work here present would not be possible without your trust in this project, your help and constant motivation to do better.

I also want to thank:

To my Mother, for being my role model.

To my Father, for always supporting my dreams.

To Tiago, my true partner in life, in every way.

To Tiago's parents, for being the family I got the luck to join.

To my Grandmother, for her love.

To my Grandfather, for his protection.

And, last but not least, to Eva, Sara and Laura, for always being there!

Resumo

Introdução: O sector da saúde é fortemente afetado pelo cibercrime, com as principais técnicas de ataque a serem direcionadas para os utilizadores. Por isso, os profissionais de saúde têm um papel fundamental na minimização destes ataques, quando devidamente treinados. As estratégias de formação gamificada em cibersegurança têm resultados bastante positivos ao nível da aquisição e retenção de conhecimento, tendo vantagens ao nível da gestão dos recursos e do tempo.

Objetivos: Descrever o estado da arte relacionado com o impacto da cibersegurança no sector da saúde e com a gamificação; identificar os componentes associados ao desenvolvimento de soluções de gamificação; comparar as plataformas de gamificação existentes; definir uma metodologia de gamificação adequada para a formação em cibersegurança de profissionais de saúde e desenvolver uma ferramenta de gamificação para a sensibilização em cibersegurança de profissionais de saúde.

Metodologia: Desenvolveu-se uma metodologia de gamificação para a formação em cibersegurança dos profissionais de saúde. Foi igualmente desenvolvido um protótipo da estratégia de formação gamificada, específica para o setor da saúde, onde consta um piloto da aplicação (Health-Cy-Game).

Resultados: Desenvolvimento do protótipo da estratégia de formação gamificada – Health-Cy-Game – de acordo com o perfil de conhecimentos estabelecido: conhecimento geral de tecnologia; autenticação e gestão de palavras-passe; técnicas de ciberataques dirigidas ao sector da saúde; gestão da informação; manutenção e atualização de *software*, e procedimentos e regulamentos em cibersegurança das instituições de saúde.

Disposições finais: No setor da saúde, a cibersegurança deverá constituir uma preocupação central dos planos estratégicos de segurança e qualidade dos cuidados. Para atingir este estado de segurança, é preciso munir os utilizadores da tecnologia de conhecimentos adequados. “Health-Cy-Game” foi construído tendo em conta o perfil de competências destes profissionais e as especificidades deste sector, de acordo com o Referencial de Competências e Conhecimentos do Centro Nacional de Cibersegurança e as escalas *Risky Cybersecurity Behaviours Scale (RsCB)* e *Security Behaviour Intentions Scale (SeBIS)*.

Palavras-chave: cibersegurança, saúde, gamificação, formação

Abstract

Introduction: The healthcare sector is heavily affected by cybercrime, with the majority of techniques used being address to its users. Health professionals have a key role in minimizing these attacks, when properly trained. Gamified training strategies in cybersecurity have very positive results in terms of knowledge acquisition and retention, with advantages in terms of resources and time management.

Objectives: To describe the state-of-the-art related to the impact of cybersecurity in the health sector and with gamification; identify the components associated with the development of gamification solutions; compare existing gamification platforms; define an appropriate gamification methodology for training health professionals in cybersecurity and develop a gamification tool to raise awareness of cybersecurity among health professionals.

Methodology: A gamification methodology was developed for training health professionals in cybersecurity. A prototype of the gamified training strategy, specific for the health sector, was also developed, which contains a pilot application (Health-Cy-Game).

Results: Development of the prototype of the gamified training strategy – Health-Cy-Game – according to the knowledge profile established: general knowledge of technology; authentication and password management; cyberattack techniques targeting the health sector; information management; maintenance and updating of software, and procedures and regulations in cybersecurity of health institutions.

Final Provisions: In the healthcare sector, cybersecurity must be a central concern of strategic plans addressed to safety and quality of care. To achieve this state of security, it is necessary to provide adequate training to healthcare professionals. “Health-Cy-Game” was built taking into account the skills profile of these professionals and the specificities of this sector, in accordance with *Centro Nacional de Cibersegurança’s* roadmap “*Competências e Conhecimentos*”, the Risky Cybersecurity Behaviours Scale (RsCB) and Security Behaviour Intentions Scale (SeBIS).

Keywords: cybersecurity, health sector, gamification, training

General Index

1	Introduction	1
1.1	Context and pertinence of the subject	1
1.2	Goals	3
1.3	Research methodology and outcomes	4
2	Fundamentals	5
2.1	Cybersecurity	6
2.1.1	Cybersecurity in the health sector	6
2.2	Gamification	8
2.2.1	Gamification and behavioral design	8
2.2.2	Design and modelling	10
2.2.3	Implementation – benchmarking of platforms for gamification	12
2.2.4	Gamification applied to cybersecurity training and awareness	14
2.2.4.1	Type of games used in cybersecurity training	19
2.2.4.2	Game elements used in cybersecurity training	19
2.2.4.3	Game genres user in cybersecurity training	20
3	Methodology - Health-Cy-Game development	21
3.1	Cybersecurity training: the design of the conceptual map of training content	21
3.2	6D Framework	34
3.3	Defining gamification elements	39
3.4	Motivational Design – ARCS + G model	39
4	Results: Health-Cy-Game proof of concept	43
4.1	Badges and achievements	44

4.2	Management and implementation	45
4.3	Lessons (Levels)	48
4.4	Octalysis framework applied to Health-Cy-Game	64
5	Conclusions	66
6	References	69
7	Appendixes	72
7.1	Health-Cy-Game user's manual	72
7.2	Questions' database exemplification	78
7.3	Rapid Quizz question's database exemplification	79

Index of Tables

Table 2.1 – Definition of mechanisms and techniques associated with cyberattacks _____	7
Table 2.2 – Benchmarking of gamification platforms _____	13
Table 2.3 – Solutions for cybersecurity training for employees _____	16
Table 3.1 – Cybersecurity competencies suitable for healthcare workers’ profile (from CNCS’ roadmap) _____	27
Table 3.2 - Scale Items for the Risky Cybersecurity Behaviours Scale (RScB) _____	28
Table 3.3 – Security Behaviour Intentions Scale (SeBIS) divided by its 4 domains _____	29
Table 3.4 – Health-Cy-Game domains definition _____	31
Table 3.5 – Behavior of the audience _____	35
Table 3.6 - Categories of the ARCS+G model ⁴⁰ _____	41
Table 3.7 – ARCS+G model applied to Health-Cy-Game _____	42
Table 4.1 – Badges collection and description _____	44
Table 4.2 – Exemplification of Health-Cy-Game’s questions and games _____	49

Index of Figures

Fig. 2.1 – Octalysis framework design ²⁵ _____	9
Fig. 2.2 – 6D framework for the development of gamified solutions _____	11
Fig. 3.1 – Methodology used to identify Health-Cy-Game conceptual map on cybersecurity training topics. _____	22
Fig. 3.2 – Results derived of the analysis and selection of CNCS’ roadmap “Competências e Conhecimentos” _____	26
Fig. 3.3 – User’s type Hexad Scale for gamification ³⁶ . _____	36
Fig. 3.4 – Progression stairs ²³ (adapted by Ana Carreiro, 2023) _____	37
Fig. 3.5 – ARCS model (designed by Carreiro, A. 2022) _____	40
Fig. 4.1 - Character “Cy” _____	43
Fig. 4.2 – “Health-Cy-Game” logo (colored version on the left and monochromatic on the right) (designed by Carreiro, A. 2023) _____	43
Fig. 4.3 – EdApp’s performance dashboard _____	47
Fig. 4.4 – Health-Cy-Game: user’s perspective. A – Health-Cy-Game first screen; B – User profile; C – Leaderboard; D – Badges view _____	48
Fig. 4.5 – Health-Cy-Game first level home screen _____	51
Fig. 4.6 – “Cy” (character) introduction _____	52
Fig. 4.7 – Exemplification of topics presentation (A) and “alphabet soup” game (B) _____	52
Fig. 4.8 - Quem quer ser tecnológico” game template and question exemplification _____	53
Fig. 4.9 - Jeopardy Game presentation. The showed question corresponds to punctuation 400 in “PCs” category. _____	53
Fig. 4.10 – Cy presenting level 2 _____	54
Fig. 4.11 – Exemplification of short-games used to present theoretical concepts _____	55
Fig. 4.12 – Last game: “Memory Game” _____	55
Fig. 4.13 – Cy presenting level 3 _____	57
Fig. 4.14 – Image map containing the definition of the most common cyberattacks. When the user clicks on the box, the definition appears. _____	57

Fig. 4.15 – Short-game “Que ataque sou?!”	58
Fig. 4.16 – Short-game “To phish or not to phish?”	58
Fig. 4.17 – The elevator game	59
Fig. 4.18 – “Cy” presenting level 4	60
Fig. 4.19 – Theoretical topic presentation	60
Fig. 4.20 – Exemplification of the multiple-choice questions of “Protect&Defend” game	61
Fig. 4.21 – HEALTH-CY-GAME QUIZZ exemplification.	62
Fig. 4.22 – Course certificate	63
Fig. 4.23 – Health-Cy-Game: Octalysis Framework	64

Acronyms and abbreviations

CNCS - Centro Nacional de Cibersegurança

ENISA - European Union Agency for Network and Information Security

HTA - Health Technology Assessment

HW - Healthcare Workers

IoMT - Internet of Medical Things

IoT - Internet of Things

IT - Information technologies

NHS - National Health System

RScB - Risky Cybersecurity Behaviours Scale

SeBIS - Security Behaviour Intentions Scale

SPMS - Serviços Partilhados do Ministério da Saúde

WHO - World Health Organization

1 Introduction

Nowadays, technology walks side by side with medical advances and patient prognostic improvement. It can be found everywhere inside a medical facility, and it allows rapid patient identification as well as rapid access to the medical background, leading to more accurate diagnoses of pathologies and more effective treatment. However, technology development and implementation also bring some new challenges to the healthcare sector.

Over the past few years, the number of successful cyberattacks on health institutions has risen, causing interruptions in the normal functioning of healthcare facilities, therefore compromising the availability and quality of health care delivered to patients¹. In 2018, according to European Union Agency for Network and Information Security (ENISA), the healthcare sector represented 27% of the total number of cyberattacks in Europe². The health sector is an attractive target because it combines the existence of a large amount of sensitive data aligned with poor implementation of defense structures³.

Most of the cyberattacks in the health sector occur due to a low level of cybersecurity awareness by the main users of technology: healthcare workers². Consequently, the strategies to minimize cybersecurity vulnerabilities must also recognize healthcare workers, developing methods to provide effective training on cybersecurity to these professionals.

Gamification has emerged as a new tool to revolutionize training and education and has shown positive results when applied to cybersecurity training⁴. In fact, traditional training sessions are usually time-consuming, with poor results on motivation, engagement and knowledge retaining when compared to gamified strategies.

On this dissertation, it is proposed a gamified strategy to be applied to a healthcare institution, to provide cybersecurity training for health professionals.

1.1 Context and pertinence of the subject

This dissertation is integrated on the master's course of Health Management and Health Technology Assessment (HTA). This project is related to the domain of HTA. According to World Health Organization (WHO), it can be defined as the «systematic and multidisciplinary evaluation of the properties of health technologies and interventions covering both their direct and indirect consequences»⁵. Representing a major game changer in health, technology is also associated with new challenges regarding patient safety.

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. In 2021, institutions in Portugal, divided by several domains of activity, were attacked 881 times per week, representing an increase of 81% when compared to 2020. The most represented areas were Education, Health, and Public Administration⁶.

In 2017, WannaCry, a ransomware attack that affected National Health System (NHS), had an estimated cost of 105 million euros and more than 19 thousand appointments were cancelled, representing a major impact on the normal function of the United Kingdom's health system⁷. This attack affected many businesses worldwide and was caused by the download of an infected file to a computer. That file contained malware that then encrypted the files of the computer and demanded a ransom to unlock them⁸. Therefore, this attack could be prevented if the users were aware of this cyberattack technique and able to recognize it.

Healthcare professionals are trained to give the best medical treatment to patients according to their pathology. Despite being responsible for the operation of technology and depending on it to do their work, their training does not include topics on cybersecurity awareness.

To fight cybercrime in the health sector, it is vital to align cybersecurity to patient-safety initiatives, since this will mitigate commotions that may negatively affect access to care and impact patient outcomes⁹. Health institutions must cultivate a culture of patient safety regarding cybersecurity, where workers are proactive defenders of patient data⁹.

The increasing dependence of technology and construction of new daily workflows based on it, accentuate the need to take measures accounting patient's data safety. With that said, measuring the direct and indirect consequences regarding patient's data safety associated with the technology use must be a central concern of HTA and HTA stakeholders. Technology is, without doubt, allowing to treat more patients, improving diagnoses and prognosis, expanding health facilities to areas beyond its physical limits. For instance, virtual discussion rooms allow to present and discuss clinical cases with specialists all over the world. The exam's results can be accessed by practitioners inside and outside the health institution, permitting the clinical history of a patient to be more available, representing less error when emergent attitudes need to be taken. However, on the other hand, if a cyberattack occur, the costs are major. All the workflow is changed, causing disruption of care, culminating in the cancelation of appointments, surgeries and limiting patient admission to emergency care. The financial impact is very expressive as well.

Considering that the major types of cyberattacks and its techniques target humans, developing methods to raise cybersecurity awareness is vital to ensure that

increasing technology expression in health sector is accompanied by proper training of technology users: health professionals. Consequently, HTA must include procedures and protocols to ensure cybersecurity in health facilities.

Nevertheless, in a business sector that is overloaded and has low resources, the success of the training program will require the adoption of strategies adequate to its reality. Gamification is a new technique, where the user can manage their training time more efficiently, and has shown positive results in training and education, improving motivation, adherence and retaining of knowledge¹⁰. It has been used with cybersecurity training in other business areas and has shown positive results as well¹¹.

Health-Cy-Game, the prototype of the gamified cybersecurity training methodology developed in this dissertation, was constructed considering the profile of health professionals and adequate to its reality and needs. Different input and standpoints, including professionals from health sciences, education, and cybersecurity, made this a more enriched training experience and contributed to the distinction of the methodology from others already available on the market, that were not constructed to health sector specifically. With this, it is possible to ensure proper training of health professionals, making them more cyberaware and less susceptible to cyber threats, resulting in increased data safety and health sector protection from cybercrime.

This dissertation is an outcome of the project with the reference IPL/2022/HeCyGame_ESTeSL, financed by IDI&CA.

1.2 Goals

This dissertation aims to develop a gamified strategy to be used for cybersecurity training of healthcare professionals. To do so, the following specific objectives were attained:

1. To describe the state-of-the-art related to cybersecurity impact on the health sector and data safety;
2. To describe the state-of-the-art related to gamification, mentioning its advantages, highlighting its impact on education and health resources training;
3. To describe the state-of-the-art related to the application of gamification on cybersecurity training in a corporate context;
4. To identify the components associated with the development of gamified solutions;
5. To compare the available platforms on the market to the development of gamified strategies;
6. To define a gamified methodology suitable for the cybersecurity training of healthcare workers, according to their level of competencies;

7. To create a prototype of the gamified solution, implementing it on a gamification platform.

1.3 Research methodology and outcomes

To achieve the goals defined for this dissertation, the first step was to conduct a review of the literature on cybersecurity, defining the main concepts, allowing to identify the healthcare workers' profile and their level of competencies on cybersecurity, the main concepts on gamification and its application to education and cybersecurity training.

After this process, the investigation proceeded with the creation and definition of the gamified strategy, finalizing its application to a gamification platform and creation of the prototype, called Health-Cy-Game.

The results attained with this project are: 1) the definition of a cybersecurity theoretical roadmap suitable for healthcare workers' training; 2) the building of a gamified methodology for cybersecurity training in the health sector and, 3) the construction of a prototype of the gamified strategy.

To better understand the steps taken to the development of Health-Cy-Game, this dissertation was divided in four chapters. In chapter two, entitled "Fundamentals", state-of-the-art reviewing cybersecurity topics and gamification can be found. The methodology related to the game topics selection and development can be found in chapter three, "Methodology – Health-Cy-Game development". The prototype of Health-Cy-Game with its mockups is presented in chapter four, "Results: "Health-Cy-Game proof of concept".

2 Fundamentals

Associated with the technological innovation that has been verified in the past years, new concepts have emerged. Internet of Things (IoT) refers to the possibility of connecting objects to the internet and controlling them remotely, making it possible to explore new dynamics of daily basis activities¹². In the medical field, the Internet of Medical Things (IoMT) refers to the possibility to connect medical devices and applications used in healthcare to networks. One example of this reality is the medical devices controlled remotely, like implantable cardiac devices or insulin bombs¹³. This expansion has allowed the growth of telemedicine, which is crucial to the Covid-19 period but is also accompanied by new cybersecurity challenges.

With this connectivity, structures are more susceptible to cybercrime. Being connected to the internet means that there are no physical barriers to prevent the penetration and stealing of information. Attacks can emerge from anywhere around the world. Moreover, 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 between healthcare workers among different health institutions. Medical devices connected to the net are becoming more common, with proven advantages to institutions as well as for the patients, but may be at risk if a cyberattack occurs, threatening the life of its user¹⁴. This expansion of the technology use to almost every task also means that if an attack occurs, the workflow of the facility will be severely compromised, with important damage and costs.

Healthcare institutions are appealing targets to hackers, because of the amount of sensitive data they usually hold and the low investment in advanced cybersecurity infrastructures¹⁵. Being human error one of the main causes of cyberattacks, it is important to find effective strategies to raise awareness about cybersecurity's importance and pertinence in a work context.

Healthcare professionals are trained to provide the best care to their patients according to best scientific references and good practices principles. However, due to the recent advances in technology and the requirement to keep up with new workflows and new daily challenges, despite their background, healthcare workers must be trained, and human resources training programs should focus on this new paradigm. Safety, now, is not just a matter of keeping information physical restrained. New threats arise from all over the world.

But, in a sector that has limited resources and with different needs from others, how to keep up and do better? 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, such as gamification.

Gamification has emerged as an effective way of providing training and has been applied to cybersecurity training in the enterprise context, but not in the health sector so far. Health professionals have a different profile from other professions like the ones linked to IT, finance, engineering, or management. So, it is important to build a strategy that fits the healthcare workers' profile and level of competence to be successful.

In this chapter, entitled "Fundamentals", it will be presented important concepts to the development of this dissertation.

2.1 Cybersecurity

According to ISO/IEC 27032:2012, cybersecurity is the «preservation of confidentiality, integrity and availability of information in cyberspace»¹⁶. 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»¹⁶.

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 the new concept of cybersecurity culture.

The cybersecurity culture involves education programs, IT infrastructure auditing and the review of security policies to make hospital personnel's more aware when processing sensitive information in daily business operations, thus preventing attacks or leakages².

Cyber risk is defined as «operational risks to information and technology assets that have consequences affecting the confidentiality, availability, and/or integrity of information or information systems»¹⁷. A data breach is a «security incident in which sensitive, protected, or confidential data are copied, transmitted, viewed, stolen, or used by an unauthorized individual»¹⁷.

2.1.1 Cybersecurity in the health sector

In 2018, healthcare institutions represented 27% of the targets of cyberattacks in Europe². Healthcare institutions are very susceptible to cyberattacks because of the amount of sensitive data they carry¹⁵ as well as the critical character of the repositioning of the systems, making them more willing to pay the ransom in ransomware attacks, for instance¹⁸.

The major cause for those breaks is related to short levels of cybersecurity awareness by the main user of IT – humans. Consequently, security issues cannot be

addressed using only technical specifications¹⁸. Human error is associated with more than 80% of cyber incidents and malware attacks¹⁹. ENISA’s report (between January 2019 and April 2020) revealed that malware, web-based attacks, and phishing occupy the top three main causes for cyberattacks²⁰ and a total of 50,6% of attacked hospitals identified insider threats as the principal fragility in security²¹. Being the main responsible for data breaches worldwide, 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), with the goal to create a guide to improve cybersecurity on healthcare, which concluded that regular training of professionals (one session a year) significantly decreased the impact of cyberattacks¹⁴.

E-mail 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 Hospitals¹⁴ (Table 2.1). All these techniques may result from phishing or ransomware attacks and are associated with low cybersecurity awareness levels.

Table 2.1 – Definition of mechanisms and techniques associated with cyberattacks

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’s a malware that infects the computer or the network and steals the data, encrypting them, 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 on the 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 its surviving, and results by unauthorized access to its configuration, changing it and leading to inaccurate measures or treatments.

2.2 Gamification

The term “gamification” was first used in 2002 but it only became popular around 2010²². It can be defined as the use of elements typically found in game design applied to nongame situations. 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, by TalentLMS, stated that companies that apply gamification strategies reach an 89 per cent increment in their productivity, and an 88 per cent increment in employee satisfaction compared to the ones that don't recur to gamification²³.

Specifically, when talking about education and training programs for employees, about 90 per cent 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 don't match the expectations and the culture of different generations, such as the millennials and generation Z, born in the digital era. 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 engagement²³. A study developed by the Massachusetts Institute of Technology concluded that gamification training sessions led to a 90 per cent 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 processes²⁴.

2.2.1 Gamification and behavioral design

The capability of behavioral influence using gamification strategies is difficult to predict because their impact on the results depends on its adequacy to users' profiles. Gamification allows a process to be a “Human-Focused Design”, considering other aspects than pure efficiencies, such as human motivation to use it²⁵. Assessing a gamification strategy is always difficult and can lead to multiple outcomes depending on the assessor. Mostly, in a gamified environment, the evaluation must focus on the balance between the strategy and the users' expectations and motivation²³.

The Octalysis framework (Fig. 2.1) was developed to assess gamification and its influence on human behavior by Yu-Kai Chou²³ and it's the most used framework to evaluate gamification and behavioral design.

It's a result of understanding game mechanisms that kept players motivated and it's built as an octagon in which the sides represent the individual motivators, known as the core drives for gamification, in a total of eight.

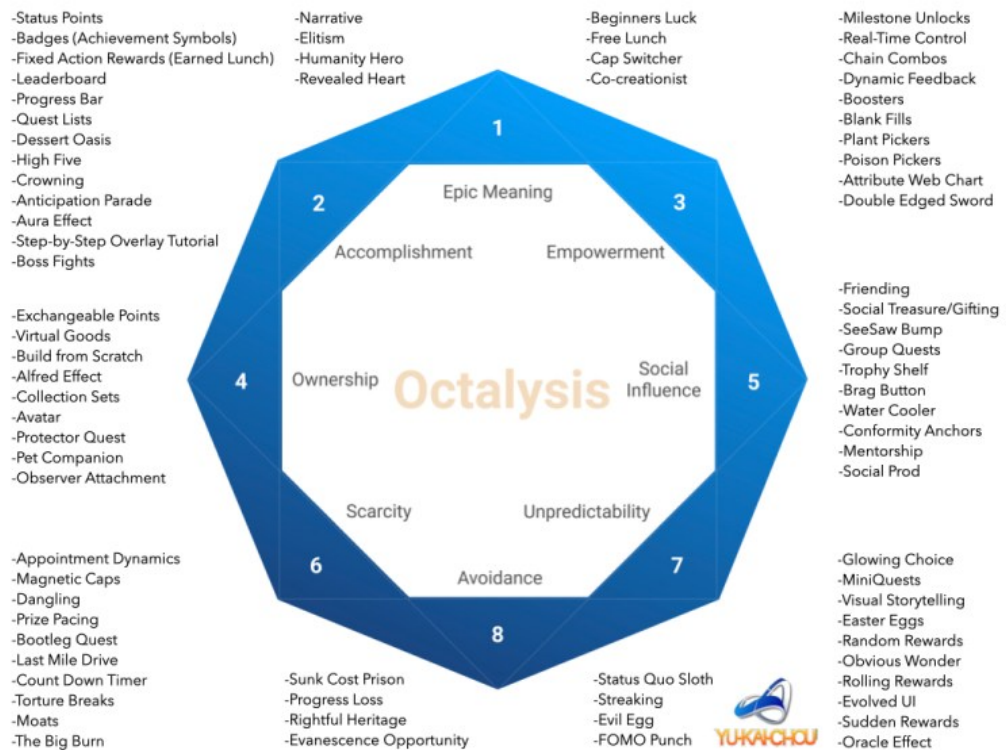


Fig. 2.1 – Octalysis framework design²⁵

The eight core drives for gamification can be defined as:

- Epic Meaning:** the player believes that he is a part of something bigger than himself and was the chosen one to complete a task. For example, this is the core motivator of blog users that spent their time for free to help the community, as seen in the big platform Wikipedia. This is also present with the feeling of “beginner’s luck.”
- Accomplishment:** it's the internal drive resulting from progress, developing skills, and overcoming challenges. A badge without a challenge is not meaningful for the player. This is the easiest aspect to design in gamification strategies since it can be obtained by implementing badges, points, and leaderboards.

- c) Empowerment: the player is engaged in the process of using their creativity to overcome game scenarios and try different combinations. The user needs to explore their creativity but receiving feedback from it is also important. For example, in a game where the user must discover the hidden key, getting the key and passing it to the next level of the game is very important.
- d) Ownership: motivation achieved from ownership makes the player always want to improve what they own. For example, if the player has an avatar that can be customizable, the tendency is to feel more engaged and motivated to keep improving their profile. This is also the drive that's present in collecting stamps and making it fun.
- e) Social influence: components such as mentorship, acceptance and competition are integrated into this core drive. Motivation is achieved by the need to get closer or overcome other people's results.
- f) Scarcity: this means to want something you can't have and can be achieved by implementing appointment dynamics, such as the need to come back later to get the reward, leaving people to think about it all day.
- g) Unpredictability: not knowing what will come next makes people want to find it out and keep engaged with the story. This is the main core drive for game addiction, and it's also present in movies.
- h) Avoidance: based on the need to avoid negative things from happening, like losing all the game's progress and it is expressed on the need to act immediately to not feel that the opportunity was lost forever.

2.2.2 Design and modelling

The most important aspect of the development of a gamified strategy is its adequacy to its users. Many taxonomy systems can be used to identify the profile of the users, but specifically, in the gamification context, Andrzej Marczewsky's is the most referenced one. It suggests there are six types of users: the entrepreneur, the socializer, the philanthropist, the "free spirit", the disruptor and the player. The profile is identified by the application of a questionnaire and relates to an Hexad scale²³. This topic will be further explored in section 3.2.

However, there are no guidelines on how to develop successful gamification strategies since it combines a variety of domains as referred before. Despite that, many frameworks can be successfully used to develop gamification strategies. The most popular is **framework 6D**, developed by Kevin Werbach, characterized by six steps (Fig. 2.2)²³.

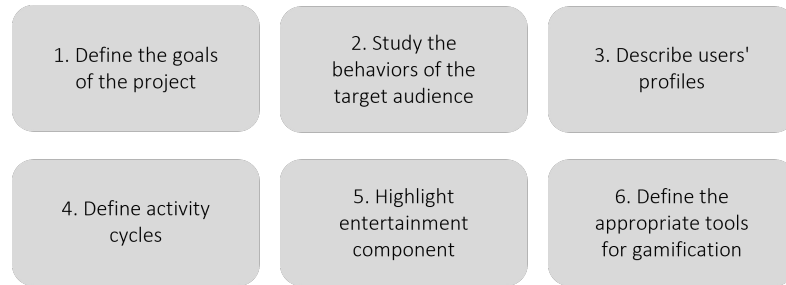


Fig. 2.2 – 6D framework for the development of gamified solutions

To define the goals of the project, the question “*what do I expect with the implementation of this gamified solution?*” must be answered. The next step, to study the behaviors of the target audience, relates to define what the users will do (the interactions between the user and the interface) and how it will be measured, establishing a connection between the activities and their metrics. For instance, the points that a player earns after completing a challenge, explores the attitude – complete the challenge – and how the system reacts to it: by earning points.

Since every person is different and has different beliefs and expectations, the use of game mechanics and elements for the reward system should be personalized. To do so, the taxonomy system developed by Andrzej Marczewsky relates the type of player with the elements that best work for them. Then, the definition of the activity cycles (the engagement and progression cycles) is very important and relates to motivational design. With this, entertainment component may then be taken into count. Entertainment, when talking about a gamified experience, is also a very important part to consider. In fact, engagement, and motivation result from the capacity the game has to affect the players, the capacity to make them experience new feelings and sensations. The appropriate tools for gamification relate to the design and modelling, the implementation, and the assessment. The implementation of a gamification strategy can be made mostly in two ways: the team can select a gamification platform that has already been launched and adapt it to the concept of their project, or it can be created from scratch. This last option requires a team of software engineers and is more time-consuming. Choosing a platform that is already launched has some vantages since the game objects and mechanics have already been validated. However, it will have limited personalization options and the users must be sure that the selection of the platform matches the goals of the project. In the end, assessing a gamification strategy is always difficult and can lead to multiple outcomes depending on the assessor. The 6D framework will be more explored and detailed later in this dissertation, in section **3.2**.

Mostly, in a gamified environment, the evaluation must focus on the balance between the strategy and the users’ expectations and motivation. Some frameworks,

such as framework Octalysis described in section **2.2.1**, were developed to assess gamification, by Yu-Kai Chou.

2.2.3 Implementation – benchmarking of platforms for gamification

Multiple platforms exist in the market to allow gamification and make it more easily implementable. Some solutions allow the full personalization of popular games and others consist of specific solutions developed and explored by some companies, not allowing customization, being the statistics of use and the availability managed by the company. All the most used platforms for the development of gamification strategies were considered and were compared in terms of costs, operating on a mobile app easily available for users, its application for training purposes, customization, and game options. The analysis is summarized in Table 2.2.

Some available solutions, such as Badgeville, only allow the management of scores and statistics and not the development of fully gamified strategies. Gametize, Gamify and EdApp are platforms that allow the adaptation of popular games, such as crosswords or “Candy Crush Saga”, without having to fully code it. EdApp is easier to work with and it offers a lot of resources for free. It is free to create the gamified solution and the payment will allow access to more advanced features such as badges and other gamified items. Those platforms easily allow integration with mobile apps and online games. It allows the integration on mobile systems, tablets and computers, this last one using its online version. SoSafe is a company that sells gamified approaches for cybersecurity awareness and training, but there are no specific solutions for the healthcare industry and the app is not customizable. UStream is also a company that sells “InfoSec”, a gamified approach to information security training as well. But, as SoSafe, this is not directly designed for healthcare workers.

Moreover, Microsoft, with Azure PlayFab, Google, with Google Play Services, and Amazon, with Amazon Game Sparks, allow the integration of developed games into those platforms, with access to multiple resources, some of them for free. However, to use it, knowledge and application of coding language are required.

Table 2.2 – Benchmarking of gamification platforms

Platform	Price	Interfaces available	Game customization	Observations	Access link
Gametize	100 USD/month	T/A/D	Yes		https://gametize.com
Gamify	79 USD/month	T/A/D	Yes		https://www.gamify.com
EdApp	Free/1,95 USD/active user/month	T/A/D	Yes		https://www.EdApp.com/
Sosafe	Information not publicly available	Information not publicly available	Information not available	Solutions designed specifically for cybersecurity, not customizable	https://sosafe-awareness.com/
Qstream	Information not publicly available	T/A/D	Information not publicly available	InfoSec – game designed for information security training https://qstream.com/content-library/information-technology/	https://qstream.com
Kahoot!	72 EUR/year	T/A/D	Yes		https://kahoot.com/
Edgagement	Information not publicly available	T/A/D	Yes		https://edgagement.com/
Archy Learning	100 USD/month	T/A/D	Yes		https://archylearning.com/
Mambo.IO	Information not publicly available	T/A/D	Information not publicly available		https://mambo.io/
Bunchball Nitro	Information not publicly available	T/A/D	Information not publicly available		https://www.biworldwide.com/

Legend: T – Android platforms; A – Apple platforms; D – Desktop/website platforms

2.2.4 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 employees²⁶. 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 elements²⁴ while promoting active learning and increasing retention of the learnt skills in comparison to traditional learning approaches²⁷.

The main purpose of this dissertation is to develop a strategy that can be applied to the healthcare sector, therefore to the employees of an organization. Due to that fact, this analysis will only include the existing solutions whose target audience includes employees (Table 2.3).

Cybersecurity awareness training should focus on real-life threats. Therefore, the main topics addressed in cybersecurity training are password management, malware and spam, patch management, and phishing techniques²⁸.

CyberNEXS is used for professional certification in cybersecurity, and it's considered the standard in cybersecurity training due to its large-scale implementation and use. Micro Games, developed by Wombat, consist of a series of multiple short games targeting one of the main topics in cybersecurity training, such as, for example, the "Anti-Phishing Pill" game. "Game of Threats", developed by PMC, is one of the most complete solutions regarding the theoretical concepts it includes. "CyberProtect", on the other hand, is one of the games that include less cybersecurity topics, focusing only on basic knowledge.

Even though there are multiple choices available, we couldn't find one specifically addressed to the healthcare industry. Healthcare workers are trained to provide the best care for their patients and have low awareness levels of cybersecurity²⁹. Finding the finest strategies to implement a training program on cybersecurity is therefore crucial and must handle time and resources in the most efficient way possible.

DeCarlo et. al applied a gamified training on cybersecurity to a sample of healthcare workers and concluded that gamification training conducted to more cybersecurity awareness and high levels of reported incidents to IT when compared to traditional training³⁰. Considering the impact that cyberattacks have on the functioning of healthcare organizations, reducing their probability of success by training the most factor for it – humans – is vital.

Despite the fact there are multiple gamified solutions currently available and applied to cybersecurity training, the majority are paid and targeted to specific clients such as finance or engineering field. It was not possible to find one available and suitable for the level of knowledge of healthcare workers. Moreover, the free-to-use ones are very simple, targeting children and the general audience, focusing on general cyber awareness, not focusing on the problems of the healthcare sector as well. So, with this work, it will be developed a solution that is free, specific for health sector and easy to use independently of the cybersecurity awareness levels of the intervenients.

Cybersecurity awareness is one of the most approached subjects in the solutions previously presented. Besides that, basic technical knowledge and cyberattack techniques are also very common themes as well. The presentation of the solutions varies from simple card games to more developed 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 project.

Table 2.3 – Solutions for cybersecurity training for employees

Game name	Cybersecurity topics	Platform	Reference
What.Hack	Phishing emails	Computer game	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
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
IoT-Poly	Risk identification Risk analysis Risk evaluation	Card game	Omiya T, Fall D, Kadobayashi Y. IoT-Poly: An IoT security game practice tool for learners motivation and skills acquisition. ACM Int Conf Proceeding Ser. 2019
Cyber CIEGE	Cybersecurity definitions Information value Access control Social engineering Malware Data protection Physical security	Computer game	https://nps.edu/web/c3o/cc_intro
SoSafe (Risk & Reporting Cockpit; Intelligent Micro-Learning and Strategic Risk & Reporting Cockpit)	Cybersecurity awareness	Computer game	https://sosafe-awareness.com/
Cyber Security - Requirements Awareness Game	Network security Physical security Social engineering	Board game that uses a floor map Cards	Yasin A, Liu L, Li T, Fatima R, Jianmin W. Improving software security awareness using a serious game. IET Softw. 2019;13(2):159–69.

Secu-one	Cybersecurity threat analysis Cybersecurity incident handling Cybersecurity countermeasures assessment	Card game	Omiya T, Kadobayashi Y. Secu-One. In: Proceedings of the 2019 7th International Conference on Information and Education Technology - ICIET 2019 [Internet]. New York, New York, USA: ACM Press; 2019. p. 259–68. Available from: http://dl.acm.org/citation.cfm?doid=3323771.3323792
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/uk/en/assets/CS/Got-linkdin-v1.0.pdf https://www.pwc.com/uk/en/services/consulting/cybersecurity/game-of-threats.html
Serious Gaming: The Security Awareness Escaperoom	Phishing emails Data classification Social Engineering Secure passwords Secure Wi-Fi use Secure device handling Data sharing Dumpster driving	Escape room	https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-cyber-risk-the-security-awareness-escape-room.pdf
CyberAWARE	Phishing simulations Awareness training Cyber security toolkit	Desktop and mobile app	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.
Cyber Security Tycoon	Cyber security awareness	Mobile app	https://play.google.com/store/apps/details?id=com.AdrianKopec.CyberSecurityTycoon&hl=en_US&gl=US
Interland – Be internet awesome	Cyber security awareness	Online game	Google https://beinternetawesome.withgoogle.com/en_us/interland

WebME	Cybersecurity awareness	Mobile app	https://play.google.com/store/apps/details?id=com.thunkable.android.mrigankpawagi.WebME&hl=en_CA&gl=US
SpaceShelter	Cybersecurity awareness	Online game	https://spaceshelter.withgoogle.com/
CounterMeasures	Basic knowledge	Desktop app	Jordan, C., Knapp, M., Mitchell, D., Claypool, M., & Fidler, 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
CyberNEXS	System assessment Penetration prevention	Desktop app	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
CyberProtect	Basic knowledge	Desktop app	Labuschagne, W. A., Veerasamy, N., Burke, I., & Eloff, M. M. 2011. Design of Cyber Security Awareness Game Utilizing a Social Media Framework. In Information Security South Africa, 1–9. Johannesburg, SA: IEEE. http://dx.doi.org/10.1109/ISSA.2011.6027538
NetWars	System assessment Penetration prevention	Desktop app	SANS. 2015. NetWars. SANS Institute. Accessed January 10, 2015: http://sans.org/netwars
Micro Games (Ex. Anti-Pishing Pill)	Basic knowledge Penetration detection Password management	Desktop app	Wombat. 2015. Security Education Platform. Wombat Security Technologies. Accessed January 10, 2015: http://wombatsecurity.com/security-education
Defend the Crown	Basic knowledge on technology and cyberattack most common techniques	Mobile app	https://www.cisa.gov/cybergames

2.2.4.1 Type of games used in cybersecurity training

Gamification used in cybersecurity awareness can be divided as follows⁴:

- a) Board games: those are tabletop games involving two or more players. A board game may include dice, cards, virtual money, or other token pieces representing the different players.
- b) Card games: those are played using a deck or a pack of cards identical in shape and size.
- c) Computer games: electronic games in which the player interacts using an input device (a controller, keyboard, joystick) and receives visual and audio feedback from visual display units.
- d) Escape room: the team is locked in a room and the main goal is to escape the room by completing several tasks and solving puzzles to find the hidden key.
- e) Virtual reality: it immerses players into a 3D virtual environment. It provides visual, audio, and haptic feedback.

2.2.4.2 Game mechanics used in cybersecurity training

Game elements can be defined as the components that make up a game and to its attributes. Those are the responsible for keeping games fun along with the learning aspects⁴. When specifically targeting cybersecurity training, four-game elements are highlighted²⁷:

- **Progress mechanics:** this one is related to player motivation and can be done by using progress tools such as points, leaderboards and badges.
- **Player control:** the use of a character, a third-person perspective to engage in the gamified training, usually known as an “avatar”. Research showed that the use of avatars influences behavior.
- **Problem-solving:** the identification of a shared purpose is essential in developing strong problem-solving skills that can easily translate into practical knowledge outside of the training environment.
- **Story:** the narrative used is important to create an attachment or a bond between the learner and their avatar and to motivate the learner to keep playing.

Besides those four game elements and based on the work done by Onduto et. al, several other game elements have been found crucial in cybersecurity training, such as conflict, strategy and chance, aesthetics, mystery, challenge, penalty, the opportunity of mastery and emotional content⁴.

2.2.4.3 Game genres used in cybersecurity training

Game genres allow grouping of games that have the same types or styles, being specifically useful to provide the player and creators with an idea of the nature of the game and the necessary skills to play it. Cybersecurity training usually implements multiple game genres, with a highlight on role-playing, simulation and capture the flag^{4,31}:

- **Role-playing** –requires players to assume character roles in a fictional setting and act accordingly to the game’s story. It has well-developed storylines and is played over a longer period. This genre focuses on a player’s character growth, as the game progresses players obtain more experience and capabilities, accompanied by the increased complexity of the game’s challenges (for example: a system administrator charged with the responsibility of protecting a server or hacker required to break into a system to obtain information needed to save a hostage implement role-playing).
- **Simulation** – it consists of building replicas of real-world activities in the form of scenarios for training. Uses models which are a physical, mathematical, or logical representation of a system or process. Models create a normalized view of the cyber security situations and simulations the building of scenarios that imitate attacks on infrastructure with specific security controls.
- **Capture the flag** – these games set opposing players against each other in a test of their cyber security skills. Once a challenge has solved the player or his team receives a flag which is a measure of success. These games are timed.

The development of a gamified solution, specifically when its purpose is related to training and education, requires special attention to the application of the principles and elements explored in this section. If the methodology does not suit the goal of the strategy and is not created aligned with users’ expectations, beliefs, and profiles, then its effectiveness is compromised.

After exploring the state-of-the-art related to cybersecurity and gamification, the next step will focus on the development of the methodology explored on this thesis to derive a gamified solution for cybersecurity training of health professionals.

3 Methodology - Health-Cy-Game development

Health-Cy-Game is the name of the gamified solution developed in this project, intending to provide cybersecurity training for healthcare workers. It was decided to implement the gamified methodology on EdApp platform, since it is mostly free to use, easy to understand, and integrates the gamified strategy on different formats, such as mobile app, tablet and computers.

This chapter describes the methodology developed to design the conceptual training on cybersecurity, as well as the development of the gamified solution by the application of the 6D framework as mentioned in section 2.

3.1 Cybersecurity training: the design of the conceptual map of training content

To identify the cybersecurity conceptual topics that will be integrated into Health-Cy-Game, two major tasks were identified (Fig. 3.1). The first task allowed to identify the healthcare workers' profile related to IT usage. This was obtained with different inputs, such as national guidelines on the professional profiles of healthcare workers and the contribution of healthcare workers and cybersecurity experts. The second task consisted of the cybersecurity competencies survey, aligned with the profile established, from different inputs like CNCS' roadmap, Security Behaviour Intentions Scale (SeBIS) and Risky Cybersecurity Behaviours Scale (RsCB) and, at last, to refine the data collected, to group topics by general domains and to design the final conceptual map for Health-Cy-Game training on cybersecurity.

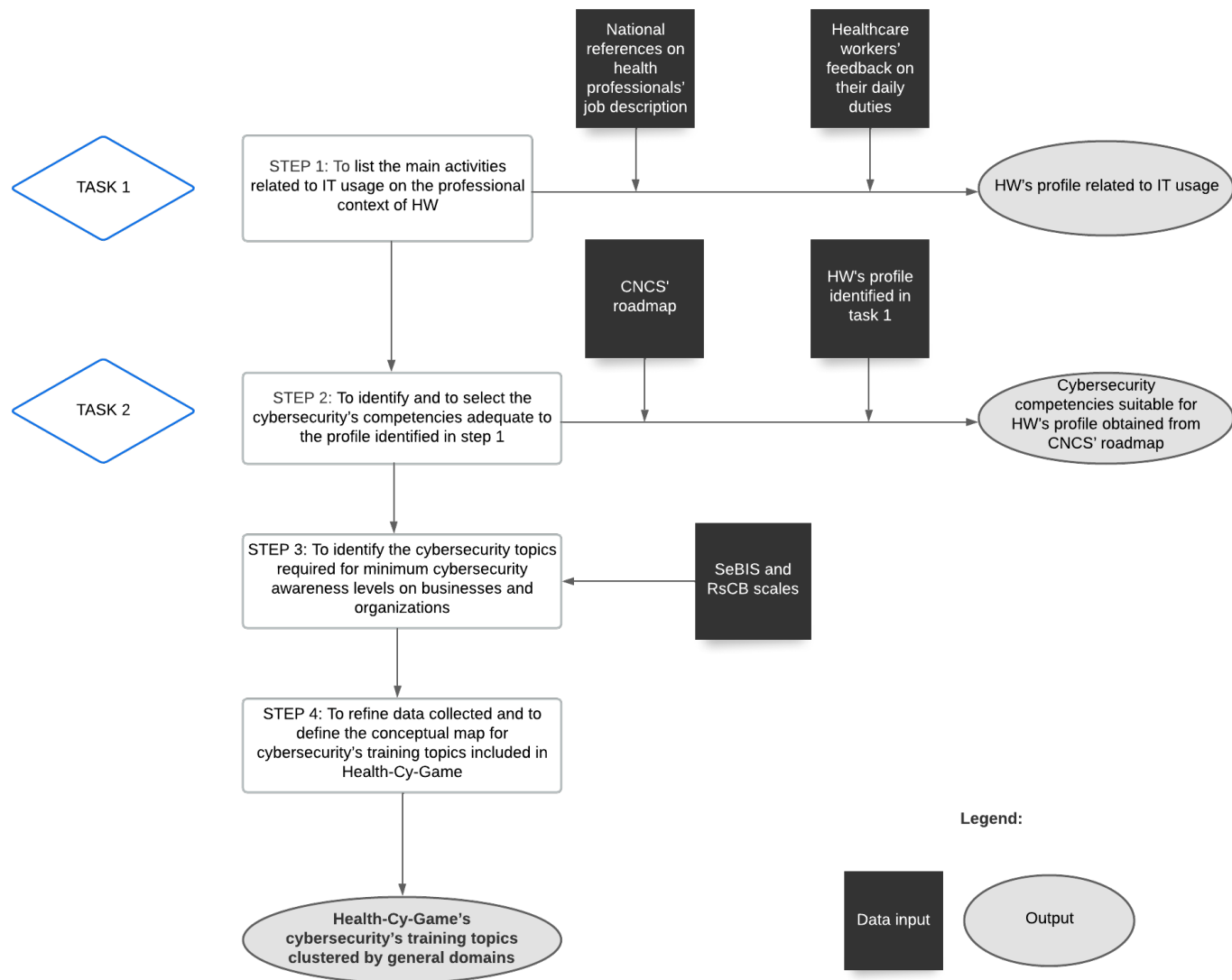


Fig. 3.1 – Methodology used to identify Health-Cy-Game conceptual map on cybersecurity training topics.

Task 1: To define healthcare workers' profile related to IT usage in their daily professional context

Healthcare professionals use technology on a daily to obtain information about patients (clinical and personal data) to provide care. Technology is associated with the recent advances in the medical field and maintaining normal activity when technology fails is becoming more challenging.

Step 1 - To list the main activities related to IT usage on the professional context of healthcare workers (HW)

In this task, it is intended to identify the main areas of knowledge associated with the tasks of healthcare workers related to their use of technology in their work context, to establish the competencies' profile. This step will allow the assortment of the cybersecurity and technology areas that must be included in the training program. To achieve this, input from different sources have been considered. National references on the description of job roles and different health professions responsibilities have been consulted, as well as input resulting from healthcare workers survey on their tasks and daily activities related to IT usage.

The team responsible for this project is multifactorial, including professionals from IT as well as from health sciences. The profile described was defined according to the contribution of their expertise and knowledge and is related to the following:

- To maintain confidentiality and use patient data according to organizational safety procedures (encryption, authentication, and access control);
- To access and use IT to obtain patient's information on health status, previous conditions, and medication, including local or national's databases;
- To use technology to examine, assess and treat diseases;
- To use digital communication platforms (e-mail, specific organization's solutions, remote meeting software)
- To upload and download data from databases.

Task 2: To map the theoretical topics suitable for cybersecurity training aligned with the healthcare workers profile established in task 1

It was not possible to find any publications defining and mapping cybersecurity topics considered the minimum level of knowledge for healthcare workers. Then, the definition of the topics that will be included in that gamified solution was based on the work from the *Centro Nacional de Cibersegurança* (CNCS) and other publications validated for other fields of business and enterprise, such as Security Behaviour Intentions Scale (SeBIS) and Risky Cybersecurity Behaviours Scale (RsCB).

Step 2 – Analyzing CNCS roadmap

CNCS is the main authority on cybersecurity in Portugal and has published a cybersecurity minimum capabilities roadmap to help to design training programs and to specify the minimum level required for cybersecurity job roles and particular education requirements³². To identify the theoretical content included in the training program, it was followed CNCS' roadmap called "*Competências e Conhecimentos*" (available from: <https://www.cncs.gov.pt/pt/referencial-de-competencias/>). This file presents as an excel table, with four columns: "domain", "sub-domain", "competencies" and "knowledge topics".

The selection and exclusion criteria were based on the profile defined in task 1. At first, it was selected the "specialized" competencies on the domain column. The domains included in this document are divided in specialized and transversals. The transversals include other areas of knowledge, such as relational competencies, leadership, and decision-making policies. Those areas are related to the soft skills needed to work in any field and are not exclusive to cybersecurity. On the other hand, the specialized domain includes topics and more specific content related to cybersecurity and that's why it was decided to filter the document and focus only on the specialized domain. The results achieved from CNCS roadmap are described in Fig. 3.2.

The exploring of the roadmap then proceeded to the sub-domain column. The document includes four sub-domains for specialized domain: risk management, incident management, technical and organizational. Then, each sub-domain divides in competencies and each competence includes several knowledge topics, which were analyzed one by one and selected according to its best match to the profile defined in task 1.

Starting with "risk management", there is only one competence included in this sub-domain, also called "risk management". Therefore, it was only possible to select one competence for this sub-domain and, analyzing the knowledge topics included, according to the profile established in task 1, it was possible to select two knowledge topics in a total of sixteen (Table 3.1). Now, for the sub-domain "incident management", there is also just one competence: "incident management". From this section, one knowledge topic was selected in a total of seventeen. On the "technical" sub-domain, there is a total of fourteen competencies and nine of them were selected. "Forensic Analysis", "Cryptology", "Software Development", "Databases management" and "System testing" were excluded because the knowledge topics here included are more specific and directed to IT workers, requiring a more advanced level of proficiency in cybersecurity. After that, the analysis continued to the knowledge topics selection for each of the competencies included in the "technical" sub-domain and 28 knowledge topics were identified on a total of 208 possible options (Table 3.1).

At last, for the “organizational” sub-domain, four competencies were selected in a total of eleven. For those four competencies, ten knowledge topics in a total of forty-nine were selected.

Step 3 – Other references (SeBIS and RScB scales)

Serge Egelman and Eyal Peer developed the SeBIS scale (Table 3.3), in cooperation with American cyber experts and local forces, which analyzes four domains: device securement, password generation, proactive awareness and updating³³. This scale can be used for various purposes, including to help organizations identify prevalent weaknesses that could benefit from targeted interventions and to increase the effectiveness of organization training intended to enhance end-user security behavior³³. Moreover, we considered a different scale partially derived from this one - RScB – with input from Digital Forensic investigators and Law Enforcement. This scale includes behaviors that make companies more susceptible to cyberattacks (Table 3.2)³⁴.

Both SeBIS and RScB scales were developed by cybersecurity experts and are designed for enterprise environments, defining the domains on which cybersecurity training for employees must focus, as well as the risky behaviors that may lead to a successful cyberattack. Consequently, the decision to include those scales on the roadmap for the definition of the training topics for Health-Cy-Game was based on their validation and recognition as integrating important topics for organizational cybersecurity awareness levels, being a validated method, developed by experts. Those scales were particularly useful to refine healthcare workers’ profile and cybersecurity topics that are more adequate to it.

Those scales were built by the combined work of cybersecurity expert forces and designed for enterprise environments. Even though it is not specific to healthcare, the construction of these scales allowed the definition of the basic topics that non-IT workers from the general business must have to guarantee cybersecurity. Looking at the health sector as a business and as a company that work to assure profits (the improvement of the health state of a general population), those scales can also be applied to the healthcare sector, guiding the topics that must be addressed when talking about cybersecurity awareness: password management, devices, proactive awareness and updating.

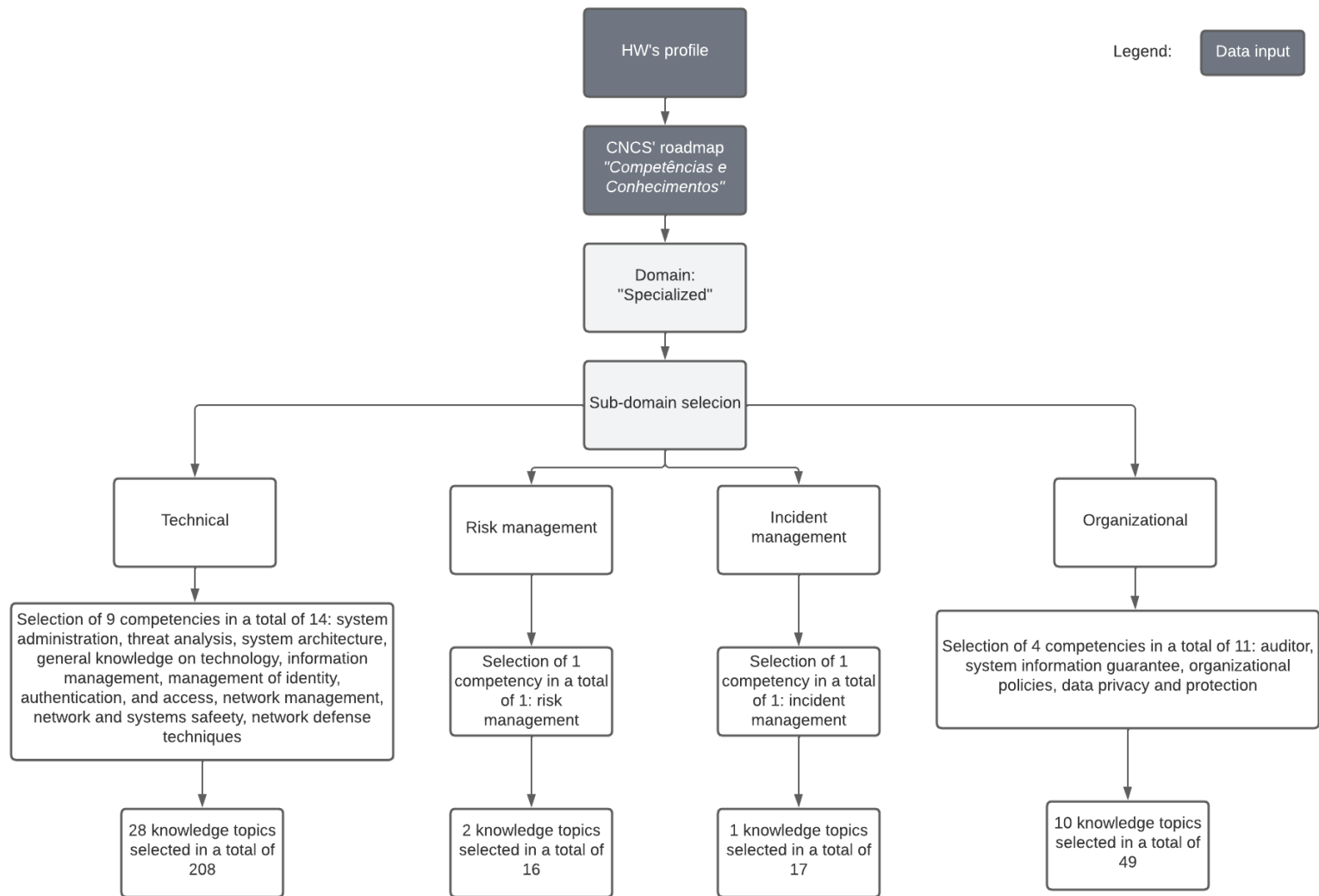


Fig. 3.2 – Results derived of the analysis and selection of CNCS' roadmap “Competências e Conhecimentos”

Table 3.1 – Cybersecurity competencies suitable for healthcare workers' profile (from CNCS' roadmap)

Competencies	Knowledge
System administration	Tools and techniques to defend and strengthen a system
Threat analysis	Techniques used to communicate with targets Behaviors associated with suspicious or abnormal activity Concepts and methods associated with malware Strategies used to collect information
System architecture	Electronic devices and its components (computer components, webcams, scanners)
Auditor	Identify cyber threats and vulnerabilities Identify the most common computer and network infections and its methods
General knowledge on technology	Functionalities associated with content creation (social media, social networks, wikis) Identify the physical components of a computer and its functions Identify the basic computer's operations Software products used in cybersecurity Emerging technologies with cyberattack potential
System information guarantee	Principles of cybersecurity and privacy and organizational requirements Principles of cybersecurity used to manage risks associated with use, processing, storage, and data transmission Principles and requirements associated with confidentiality, integrity, and availability
Information management	Data bases, portals, and ways to disseminate information Technologies associated with virtual and local data storage
Management of identity, authentication, and access	Policies and procedures associated with correct use of IT (e.g., passwords)
Network management	Good practices associated with hardware and software maintenance
Risk management	Mitigation effects strategies How to report situations associated with risk management
Incident management	Communication tools to report incidents, including internal and external entities
Organizational policies	Organization security policies

Data privacy and protection	Laws, requirements, and good practices associated with data protection and privacy Safety measures associated with health data safety Measures and good practices associated with identification of personal and sensitive data
Network and systems safety	Basic knowledge on defense network systems (e.g., firewalls, authentication)
Network defense techniques	Cybernetic terms and concepts Policies and procedures associated with cyber defense and information security Products that guarantee the safety of devices (e.g., firewall, antivirus software)

Table 3.2 - Scale Items for the Risky Cybersecurity Behaviours Scale (RScB)

Sharing passwords with friends and colleagues.
Using or creating passwords that are not very complicated (e.g. family name and date of birth).
Using the same password for multiple websites.
Using online storage systems to exchange and keep personal or sensitive information.
Entering payment information on websites that have no clear security information/certification
Using free-to-access public Wi-Fi
Relying on a trusted friend or colleague to advise you on aspects of online-security.
Downloading free antivirus software from an unknown source.
Disabling the anti-virus on my work computer so that I can download information from websites.
Bringing in my own USB to work in order to transfer data onto it.
Check that software for your smartphone/tablet/laptop/PC is up-to-date.
Downloading digital media (music, films, games) from unlicensed sources
Sharing my current location on social media.
Accepting friend requests on social media because you recognize the photo.
Clicking on links contained in unsolicited emails from an unknown source.
Sending personal information to strangers over the Internet.
Clicking on links contained in an email from a trusted friend or work colleague.
Checking for updates to any anti-virus software you have installed.
Downloading data and material from websites on my work computer without checking its authenticity.
Storing company information on my personal electronic device (e.g. smartphone/tablet/laptop)

Table 3.3 – Security Behaviour Intentions Scale (SeBIS) divided by its 4 domains

Device securement	<ul style="list-style-type: none"> • I set my computer screen to automatically lock if I don't use it for a prolonged period of time. • I use a password/passcode to unlock my laptop or tablet. • I manually lock my computer screen when I step away from it. • I use a PIN or a passcode to unlock my mobile phone.
Password generation	<ul style="list-style-type: none"> • I do not change my passwords unless I have to. • I use different passwords for different accounts I have. • When I create a new online account, I try to use a password that goes beyond the site's minimum requirements. • I do not include special characters in my password if it's not required.
Proactive awareness	<ul style="list-style-type: none"> • When someone sends me a link, I open it without first verifying where it goes. • I know what website I'm visiting based on its look and feel, rather than by looking at the URL • I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon). • When browsing websites, I mouseover links to see where they go, before clicking them. • If I discover a security problem, I continue what I was doing because I assume someone else will fix it.
Updating	<ul style="list-style-type: none"> • When I'm prompted about a software update, I install it right away. • I try to make sure that the programs I use are up to date. • I verify that my anti-virus software has been regularly updating itself.

Step 4 – To refine the data collected and to define the conceptual map for cybersecurity training using Health-Cy-Game

To refine data selected from CNCS' roadmap and to compare it with validated scales on cybersecurity awareness topics for enterprise and business, it was cross-analyzed the domains and topics approached on SeBIS, RScB and the compilation made from CNCS to help to specify the topics for Health-Cy-Game cybersecurity (Table 3.4).

Analyzing this table, it's possible to conclude that the topics on cybersecurity can be grouped by general domains. Despite the fact there was not possible to find specific guidelines addressing cybersecurity awareness topics relating to proficiency levels, nor one that applies to healthcare workers' profiles, our research allowed us to define the most common dimensions approached on different roadmaps, which will be considered as cybersecurity awareness minimum level: password management and authentication control, computer basics and devices, software maintenance and updating, data storage and sharing, organizational procedures and requirements on cybersecurity, cyberattacks techniques and proactive awareness. For this specific purpose, proactive awareness is related to the perception of risky behaviors that may lead to a cyberattack or information leak that may put users' safety at risk.

According to Healthcare Cybersecurity Essentials defined by Singapore's Ministry of Health, cybersecurity awareness programs should focus on password security and management, the steps to protect their login, shutting and locking the computer when leaving the working station, and using trusted connections and sites. Making sure users know how to report and are aware of the consequences of sharing personal information during online interactions and social media is also recommended, along with encouraging the users to look out for and report suspicious behaviors³⁵.

So, according to the best evidence at this point, the domains specified are up to date and align with the best evidence on cybersecurity minimum awareness levels for the profile of healthcare workers.

To sum up, the domains on which Health-Cy-Game training will focus are:

- General knowledge of technology: electronic devices, components, and computer basic functions.
- Password management and authentication control;
- Cyberattacks: most common techniques and proactive awareness;
- Data management (storage, transmission and secure management);
- Software maintenance and updating;
- Organizational procedures and requirements on cybersecurity

Table 3.4 – Health-Cy-Game domains definition

Principles from CNCSS	Items from RScB	Items from SeBIS	Domain
<p>Tools and techniques to defend and strengthen a system</p> <p>Policies and procedures associated with correct use of IT (e.g., passwords)</p>	<p>Sharing passwords with friends and colleagues.</p> <p>Using or creating passwords that are not very complicated (e.g. family name and date of birth).</p> <p>Using the same password for multiple websites.</p>	<p>I set my computer screen to automatically lock if I don't use it for a prolonged period of time.</p> <p>I use a password/passcode to unlock my laptop or tablet.</p> <p>I manually lock my computer screen when I step away from it.</p> <p>I use a PIN or a passcode to unlock my mobile phone.</p> <p>I do not change my passwords unless I have to.</p> <p>I use different passwords for different accounts I have.</p> <p>When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.</p> <p>I do not include special characters in my password if it's not required.</p>	<p>Password management and authentication control</p>
<p>Electronic devices and its components (computer components, webcams, scanners)</p>			<p>Computer basics and devices</p>
<p>Good practices associated with hardware and software maintenance</p>	<p>Checking for updates to any anti-virus software you have installed.</p>	<p>When I'm prompted about a software update, I install it right away.</p>	<p>Software maintenance and updating</p>

<p>Basic knowledge on defense network systems (e.g., firewalls, authentication)</p>	<p>Checking that software for your smartphone/tablet/laptop/PC is up-to-date.</p>	<p>I try to make sure that the programs I use are up to date. I verify that my anti-virus software has been regularly updating itself.</p>	
<p>Data bases, portals, and ways to disseminate information</p> <p>Technologies associated with virtual and local data storage</p> <p>Principles of cybersecurity used to manage risks associated with use, processing, storage, and data transmission</p>	<p>Storing company information on my personal electronic device (e.g. smartphone/tablet/laptop)</p> <p>Bringing in my own USB to work in order to transfer data onto it.</p> <p>Using online storage systems to exchange and keep personal or sensitive information.</p>		<p>Data storage and sharing</p>
<p>Laws, requirements, and good practices associated with data protection and privacy</p> <p>Safety measures associated with health data safety</p> <p>Measures and good practices associated with identification of personal and sensitive data</p> <p>How to report situations associated with risk management</p> <p>Organization security policies</p> <p>Communication tools to report incidents, including internal and external entities</p>			<p>Organizational procedures and requirements for cybersecurity</p>

<p>Functionalities associated with content creation (social media, social networks, wikis)</p> <p>Emerging technologies with cyberattack potential</p> <p>Techniques used to communicate with targets</p> <p>Policies and procedures associated with cyber defense and information security</p> <p>Behaviors associated with suspicious or abnormal activity</p> <p>Concepts and methods associated with malware</p> <p>Strategies used to select targets</p> <p>Strategies used to collect information</p> <p>Identify cyber threats and vulnerabilities</p> <p>Identify the most common computer and network infections and its methods</p>	<p>Sharing my current location on social media.</p> <p>Accepting friend requests on social media because you recognize the photo.</p> <p>Sending personal information to strangers over the Internet.</p> <p>Entering payment information on websites that have no clear security information/certification</p> <p>Using free-to-access public Wi-Fi</p> <p>Downloading free antivirus software from an unknown source.</p> <p>Disabling the anti-virus on my work computer so that I can download information from websites.</p> <p>Downloading digital media (music, films, games) from unlicensed sources</p> <p>Clicking on links contained in unsolicited emails from an unknown source.</p> <p>Clicking on links contained in an email from a trusted friend or work colleague.</p> <p>Downloading data and material from websites on my work computer without checking its authenticity.</p>	<p>When someone sends me a link, I open it without first verifying where it goes.</p> <p>I know what website I'm visiting based on its look and feel, rather than by looking at the URL</p> <p>I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon).</p> <p>When browsing websites, I mouseover links to see where they go, before clicking them.</p> <p>If I discover a security problem, I continue what I was doing because I assume someone else will fix it.</p>	<p>Cyberattacks techniques and proactive awareness</p>
---	---	--	---

3.2 6D Framework

As mentioned before in section 2, various frameworks can be used to build a gamified strategy. Health-Cy-Game was built following the 6D framework (Fig. 2.2). This allows the correct definition of the goals, and the behavior of the audience, to describe users' profiles, to define activity cycles and the appropriate tools for gamification, as well as highlight entertainment component.

On the following section, the application of the 6D framework to design Health-Cy-Game will be explained. To begin with, the goals of the project will be defined, a crucial step to adequate the gamified strategy to its purpose. Then, the audience's behaviors – how the users will interact with the system and how it will react – will be explored, as well as the definition of the user's profile. After this, it is possible to focus on the study of the activity cycles, along with entertainment component and the selection of gamification elements.

1. Define the goals of the project

- To improve cyberawareness of healthcare workers (to mitigate the potential and the number of cyberattacks succeeded);
- Empower healthcare workers as cybersecurity agents of health institutions;
- Match the level of cybersecurity knowledge of healthcare workers despite their background;
- Improve the attitude towards training programs developed by the organization;
- Motivate and engage users to complete the training program.

2. Study the behavior of the target audience

This step intends to define the expected users' behaviors, what the users will do and how it will be measured. According to the project's main goal, the users will have to engage and complete a gamified training program on cybersecurity. The training will be divided into lessons with different levels of complexity and different theoretical aspects, with different actions corresponding to different measures of the system (Table 3.5).

Table 3.5 – Behavior of the audience

Player's actions	System measurements
Login in the gamification platform Login daily in the gamification platform	The user will be rewarded with badges. The user will receive 2 stars per day, if he logs in.
Complete the training program: <ul style="list-style-type: none"> - Level 1/Lesson 1 - Level 2/ Lesson 2 - Level 3/ Lesson 3 - Level 4/ Lesson 4 	Total of 400 points + stars Achievements' badges (a total of 17) Maximum score: 100* + 24 stars Maximum score: 100* + 20 stars Maximum score: 100* + 17 stars Maximum score: 100* + 8 stars**
Participate on the discussion forum	
Engage on social learning – complete the lessons as a group	
Complete the extra challenge - Rapid Refresh Quizz	A different leaderboard depending on the Rapid Quizz score

*the score is automatically attributed by EdApp considering the points achieved in the game. The points are also allocated by EdApp.

** level 4 is not completed at the moment, as will be discussed further on this document (section 4).

The levels of the game – also referred as lessons due to the terminology used on the EdAapp platform - will be composed of some theoretical exposition and rapid games, such as “True or False”, “Alphabet Soup” and “Memory Game”.

The “victory state” will be defined by two types of victory defined in gamification. There will be temporal victory, achieved by the completion of extra challenges that will allow the user to have extra points, like the rapid quizz, and long-term victory, resulting from the points achieved by the completion of one level.

3. Describe users' profile

The users will be healthcare workers from different professions (nurses, doctors, allied professionals, and operational assistants), male and female, with different levels of IT proficiency. They will mostly have higher education degrees in the medical sciences, or, specifically for operational assistants, there can be users that have completed the minimum

education level (high school) according to Portuguese legal requirements for job access. The users will all be older than 18 years old, according to the minimum age required to work in Portugal.

To select the users' profile, it is recommended to use a taxonomy such as the one presented in section 2.2.2, developed by Andrzej Marczewsky. This taxonomy system attempts to map the personality types and user's traits, associating it with different six motivators in an Hexad Scale (Fig. 3.3). This is done by the application of a 24-items survey, constructed as a Likert scale, scoring users' preferences, and matching them with the motivators included in the taxonomy system³⁶.

This project did not select a sample of healthcare workers to apply the gamified solution here developed, since it was not the goal. Therefore, the game will be developed addressing the user type "player", because the success of the implementation of a gamified strategy is associated, in most people, with the use of the rewarding system. The "player" user style is defined by its will to achieve points related to its performance. This user is motivated by winning, competition, leadership, creating and personalizing. The gamification elements more suitable to this type of user are the points, rewards, leaderboards, badges, and challenges²³.

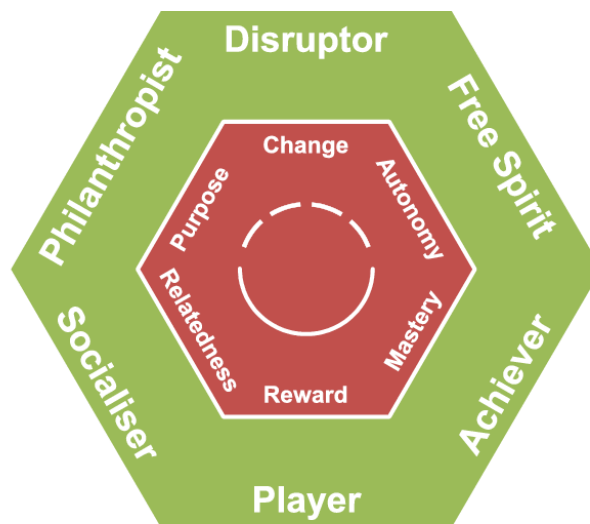


Fig. 3.3 – User's type Hexad Scale for gamification³⁶.

In the middle, colored in red are the the six motivators; on the outside area (painted in green) there is the user type classification.

4. Define activity cycles

The activity cycles on a gamified solution must align with the motivation aspects of it. The progression should not be a linear process since this might contribute to frustration and abandonment of the training. On gamification, two main activity cycles groups can be defined:

- **Engagement cycles:** micro perspective (what users do, why they do it and how the system reacts to it).
- **Progression cycles:** macro perspective about the journey, organized by a bunch of intermedial challenges to get to the main goal.

The two connect to establish the best method to guarantee motivation, along with the increasing level of competence and challenge. Engagement cycles must be related to the three main areas of motivational design: motivation, action, and feedback. So, it is important that after an important interaction between the user and the system, it gives some feedback about the user's performance through points or badges. This will increase the user's engagement and motivate him to a new action, in a new cycle, progressing into the experience.

Progression cycles are made of different game phases to keep the player motivated. In phase 1 – called onboarding – the difficulty should be low and the feedback constant. Phase 2 – middle challenge – requires a higher level of difficulty to keep the user engaged. Phase 3 – rest – allows the user to relax a bit before facing the real challenge: the boss battle. After this, a new cycle begins (Fig. 3.4)²³.

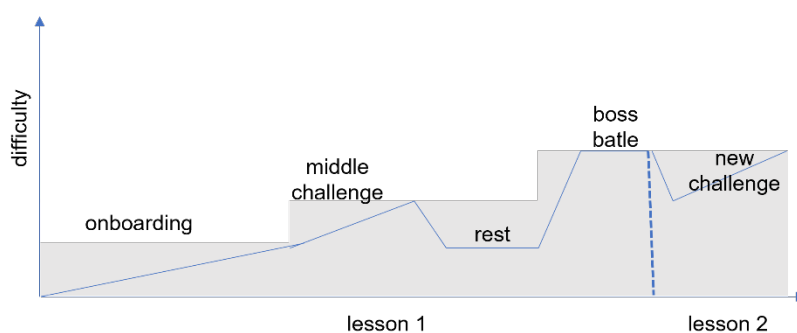


Fig. 3.4 – Progression stairs²³ (adapted by Ana Carreiro, 2023)

In the specific case of Health-Cy-Game, the engagement cycles will correspond to the earning of badges, for instance, after the first login, the completion of the first lesson, and the badges and stars achieved by several logins or hours spent training.

The progression cycles will correspond to different lessons organized by the topics described in section 4.1. The first part will be composed by general aspects of the subject, such as definitions and general knowledge questions, the second part will be questioned more specific and real scenario simulations, then the difficulty will decrease and, in the end, there will be an assessment of the knowledge obtained on the lesson, with a higher difficulty level

compared to the previous elements. For each correct and incorrect answer, user will receive reinforcement and motivation to keep playing.

The user will only have access to the next lesson if they score more than 75% of the total score possible on each level (100). The points are not cumulative, which means that to proceed with the game, the player must score at least 75% of the maximum score for each level.

EdApp automatically divides the points for the questions to obtain a maximum score of 100%. This means that a player must score at least 75% to pass to the next level. If he does not accomplish the minimum score, the player will have to retry the same level, but the game is defined to only allow the retry after 5 minutes of the first trial has a penalty, also considered a game element.

To increase engagement and knowledge retention, once the course is finished, there will be the application of a rapid quiz game (HEALTH-CY-GAME QUIZZ), that will allow the user to compete again, earning more points that will correspond to a different leaderboard.

5. Highlight entertainment component

In a gamified environment, entertainment can be defined as «pleasurable engagement, establishing a different distinction between esthetics and the more passive entertainment»²³. The “8 kinds of fun” is one of the taxonomy methods used to define the entertainment components of gamified solutions, developed by Marc LeBlanc. According to the definition associated to 8 topics (sensation, fantasy, narrative, challenge, brotherhood, discovery, expression, and submission)³⁷, the Health-Cy-Game entertainment component will be made of:

- Sensation: the game will evoke the senses of the user, using audio and visual resources.
- Challenge: the game will be composed of progressively harder levels.

6. Define the appropriate tools for gamification

The current framework will be submitted to the EdApp platform. As stated in section **2.2.2**, there are currently several platforms that allow and ease the creation of a gamified solution, not requiring special training in computer sciences. EdApp was selected because it is an open-sourced platform, available on computer and mobile platforms, very intuitive to use, that allows the total customization of the training program without requiring special training on game development. It is, however, important to acknowledge that the decision to go with an existing platform also conditionate the gamified elements available.

3.3 Defining gamification elements

Gamified strategies applied to cybersecurity training can have multiple game elements and vary on the type of game and game genre used. On Health-Cy-Game, it was chosen to develop a **computer game**, defined as an electronic game in which the player interacts using an input device. The game will be developed to be played on a mobile phone, tablet or computer.

A gamified cybersecurity training can benefit from the application of some game elements as stated in section 3.2. Aligned with the user profile (player), the elements integrated were the **progress mechanics, reward, the opportunity of mastery and visibility of progress**, related to player motivation and to the application of progress tools such as points, leaderboards, and badges.

Also, has a gamification element, is possible to find problem-solving, by the statement of cybersecurity awareness has a goal to achieve in the healthcare sector since cyberattacks cause a major loss on this sector and all technology users must act to mitigate the impact of it and, at last, the **story**. The game will be composed by a short and simple narrative, presented by the character “Cy”, to help to create an attachment between the user and the game. Penalty is another game element that can be found, consisting on the 5-minute wait between each retry after a failed attempt.

About the used game genres, it was decided to apply the casual genre type, corresponding to computer adaptation of traditional games, normally applied in cybersecurity training to train players on basic terminology and concepts⁴.

3.4 Motivational Design – ARCS + G model

At first, motivation can be defined as the «extent to which continual effort is directed towards a goal»³⁸. The success of a gamified approach to learn is deeply related to its potential to motivate users. Has seen before, motivation plays a very important role in the acquisition and retention of information. Examples of motivational features include fun activities or rewards, but their effectiveness is affected by how it allows the learner to emerge in the learning context.

The art of organizing resources to lead motivational changes is called motivational design. Motivational design can be applied to various areas such as learning and working, permitting to deploy special attributes or improve skills³⁹.

The ARCS motivational design model was designed specifically for learning environments with the intent to stimulate and sustain learners' motivation using the problem-

solving approach. More recently, its structure has been adapted to gamified learning contexts and a new model has emerged: ARCS + G model⁴⁰.

ARCS model (Fig. 3.5) is used to study the motivational stimuli to enhance learners' motivation and performance, and, in the specific context of learning, several studies have shown that ARCS design positively influences learners' motivation^{39,41}.

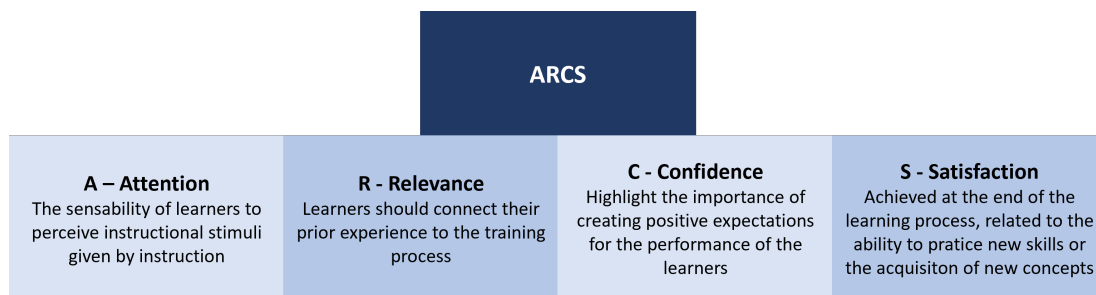


Fig. 3.5 – ARCS model (designed by Carreiro, A. 2022)

The ARCS+G (Table 3.6) resulted from an integration of game dynamics aspects on the ARCS model, such as rewards, status, competition, achievement, self-expression, and altruism according to significant characteristics between the ARCS model and gamification. The game dynamics on the ARCS+G model intend to encourage learners to explore the properties of learning strategies.

ARCS category of confidence now also integrates game dynamics related to rewards, status, and competition. A reward can be defined as something valuable that will be achieved by the player when he behaves in a certain way intending to perpetuate the player's good behavior.

Points are one example of a rewarding system that indicates progress, allowing the user to progress to the next level in the learning process. Moreover, status is also a strategy that incorporates the confidence category and is used to recognize the progression achieved. Dividing the game by different levels is one way to achieve this and can significantly improve the percentage of completion of intermediate goals in the learning process, providing progress feedback to the user.

Competition is important because it challenges the users to achieve better results by comparison of their scores with the rest of the team. Leaderboards allow the integration of competition dynamics into the gamified strategy⁴⁰.

The satisfaction category also extends to other issues related to game dynamics as well, such as achievements, self-expression, and altruism. Achievements usually encourage the players to seek challenges and set goals. Badges can be used to recognize the users' achievements and they can also integrate a social component based on the capability to share the badges on the social network.

Moreover, self-expression allows the user to have a distinct character and personality to mark his individuality. Virtually, players can create their own identity by customization an avatar using virtual goods, which can operate from the game mechanics or be purchased by the user.

Moreover, the ability to help others and offer something to others (altruism) is a great motivator to develop ongoing relationships. Gifts are a great retention tool and strong motivators, especially if the learner has a network in which the learner seeks to grow relationships⁴⁰.

Table 3.6 - Categories of the ARCS+G model⁴⁰

Model/Technique	ARCS Categories			
	Attention	Relevance	Confidence	Satisfaction
ARCS	<ul style="list-style-type: none"> - Perceptual Arousal - Inquiry Arousal - Variability 	<ul style="list-style-type: none"> - Goal orientation - Motive matching - Familiarity 	<ul style="list-style-type: none"> - Learning requirements - Success opportunities - Personal responsibility 	<ul style="list-style-type: none"> - Intrinsic reinforcement - Extrinsic rewards - Equity
Gamification	-	-	<ul style="list-style-type: none"> - Reward - Status - Competition 	<ul style="list-style-type: none"> - Achievement - Self-expression - Altruism

The motivational design of Health-Cy-Game was based on ARCS+G model (Table 3.7). The subcategory of ARCS+G “Reward” is accomplished by the point system implementation and the stars that the player can earn from each challenge.

The “status” will be showed on the main menu of the game, and the user will be able to see how many lessons have completed and the total number of lessons as well. “Competition” subcategory is achieved by leaderboards, badges, and stars. “Altruism” subcategory is incorporated with the possibility to use the discussion forum to help other learners as well as the possibility to complete lessons as a group. However, “self-expression” subcategory may only be present with the customization of the username. EdApp does not allow other forms of individual customization.

Table 3.7 – ARCS+G model applied to Health-Cy-Game

ARCS Category	ARCS+G subcategory	Process questions	Health-Cy-Game Tactics
Confidence	Reward	How can learners get rewards?	- Point system - Stars earned
	Status	How can learners know their status?	Number of lessons completed/number of total lessons in a course
	Competition	How can learners compete?	- Leaderboards - Stars
Satisfaction	Achievements	How to show the achievements of learner?	- Badges The achievements are associated with each user profile and public.
	Self-expression	How can learners show they self-expression?	- Personalized username. Other features not included due to platform (EdApp) limitations
	Altruism	How can learners be altruism?	Use discussion forum and complete lessons as a group allowing to work as a team and help colleagues.

The stars act like currency on the game. Users can use their stars to win prizes at prize draw, such as vouchers. This aims to improve competition and keep players motivated.

To assure that players keep playing, EdApp will send notifications via e-mail or push notifications, at 9 a.m and 1 p.m, reminding the need to complete a lesson. After the first login, the users will only have access to the training program for three months. In the end, the users will receive a game certificate, and the users can add the certification to their professional curriculum.

4 Results: Health-Cy-Game proof of concept

This chapter is focused on the implementation of the developed methodology on the selected platform (EdApp) and the creation of Health-Cy-Game prototype. Health-Cy-Game will start with a short story with the introduction of the characters. Cy is the robot asking for help to sensitize healthcare professionals about cybersecurity (Fig. 4.1) to protect healthcare system and mitigate the attempts of a cyberattack.

All the illustrative pictures included will represent the mobile app version, but it has been developed for desktop and tablet formats as well. The game will be developed in Portuguese.



Fig. 4.1 - Character “Cy” (design created by *upklyak* on Freepik, downloaded from https://www.freepik.com/free-vector/cute-chat-bot-cartoon-conversation-robot_6612176.htm)






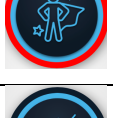

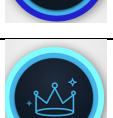
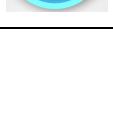
Fig. 4.2 – “Health-Cy-Game” logo (colored version on the left and monochromatic on the right) (designed by Carreiro, A. 2023)

4.1 Badges and achievements

The badges and achievements are gamified elements important for user motivation and are included on the ARCS+G model designed for Health-Cy-Game on “Satisfaction” category and “Achievements” subcategory. With badges, users will be able to show their achievements, as well as being recognized. Users may earn a total of 17 badges, according to their performance (Table 4.1). These badges include a reinforcing message.

Table 4.1 – Badges collection and description

Badge design	Title	Condition	Message associated
	Expert	To complete 1 course	You have completed the course! It's good to see you getting cyberaware!
	Achiever	To score 100% on a course	100% on a course is the true Cy way. Congratulations!
	New starter	To complete 1 lesson	A small step for men, a giant lead for cybersecurity! Keep it up!
	Enthusiastic explorer	To complete 3 lessons	Look out, it is starting to heat up, you have completed your first 3 lessons!
	True challenger	To score 100% on a lesson	You scored 100% on a lesson, keep the flow!
	Superstar	To earn 10 stars	You're a 10 out of 10!
	Cosmic	To earn 20 stars	To infinity and beyond! You're unstoppable!
	Over the moon	To earn 50 stars	You're shining with your 50 stars earned! Keep going!
	Stellar	To earn 70 stars	Oh... Look at you! Good job! You have earned 70 stars!
	Out of this world	To earn 100 stars	You have earned 100 stars; we see a bright future for you!

	Star of the show	To earn 5 stars weekly for 2 weeks	Well done is twice done! You've earned 5 stars for two weeks in a row.
	Committed learner	To open EdApp 1 time/day for 2 days.	One class a day keeps the doctor away. You logged in daily for 2 days.
	Hard worker	To open EdApp 1 time/day for 3 days	You've logged in daily for 3 days. Consistency is key, keep going!
	Continuour Improver	To open EdApp 1 time/day for 5 days	Training 5 days in a row? That's true dedication!
	Engaged Promoter	To open EdApp 1 time weekly for 4 weeks	Keep it up! You're making healthcare cyberaware!
	Consistent Champion	To open EdApp 1 time weekly for 8 weeks	A true champion! People should put a eye on you!
	Relentless Advocator	To open EdApp 1 time monthly for 3 months	This is real commitment. You are the king!

4.2 Management and implementation

To access the course, users can be invited directed via e-mail, a specific link or enter the game code corresponding to Health-Cy-Game. To implement this on an organization, inviting the users using e-mail invitation may be easier. It will be easier to training departments to reach all employees using this method, since employees are usually associated with business' e-mail addresses. On the invitation e-mail, users will receive their unique username (defined by EdApp according to user's name) as well as the password for the first login. This will limit the options to define a user's name in the game, avoiding unknown users and fake accounts. The only user's data collected by EdApp is the e-mail address, that is not public to other users, just for the manager of the application, that, in a health facility, will be the training commission. EdApp will only collect the statistics related to the training session (points, badges, number of logins per day, number of lessons or courses concluded). Other personal information will not be stored.

Statistics of users' activity, points, badges, and the leaderboard are automatically managed by EdApp and can be easily consulted on the administrator dashboard, specifically in the "Performance Dashboard" option (Fig. 4.3). This information can be exported for other

software like Excel, allowing to work and to explore the data. Information can be seen in the “overview”, or arranged by “courses”, “user groups” and “users”. On the learner’s view, the user can access leaderboard, consult the information regarding the number of stars earned as well as the badges (Fig. 4.4).

To implement Health-Cy-Game on a real-life scenario, and using EdApp, the pricing to access all the gamification features included is around 2,71€ per active user. Considering a health institution with around 2000 employees, this would cost around 5420€. EdApp offers special plans for enterprise, so it would be possible to negotiate the final cost. EdApp, however, has a free plan, but this one does not include badges and achievements. So, excluding the badges and the achievements, and keeping just the content, the leaderboard, and the stars as rewards, to implement Health-Cy-Game on a health facility would be free.

To best guide and help users through the training program, aiming to make it a full self-managed training session, the users will have a briefcase manual (appendix 7.1), available during all the training session, included on EdApp, clarifying the most important topics about the game and the game mechanics. Moreover, to increase engaging, health institutions will have a major importance on the process of implementation, requiring some marketing and publicity towards this new way of learning, starting a few weeks prior to the launching day, to get the users attention and curiosity about the game. Also, it is important to have a quick way to contact with the training commission in case users have any doubts or experience some sort of technical difficulties. It is also important to guarantee benefits to the player by completing the game. For instance, the prize draws should include attractive offers, like meal offers, or the possibility to take an extra day off.

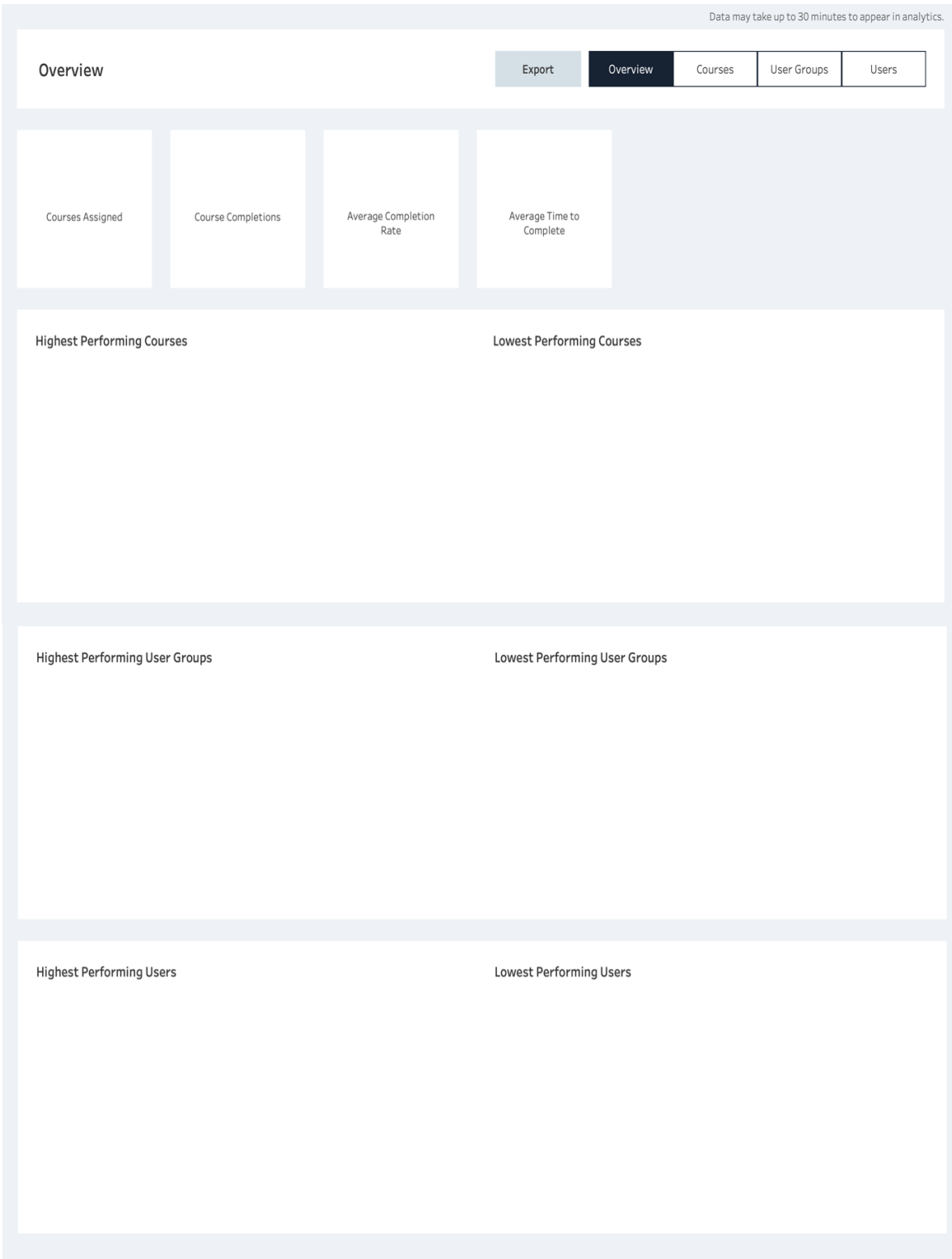


Fig. 4.3 – EdApp's performance dashboard

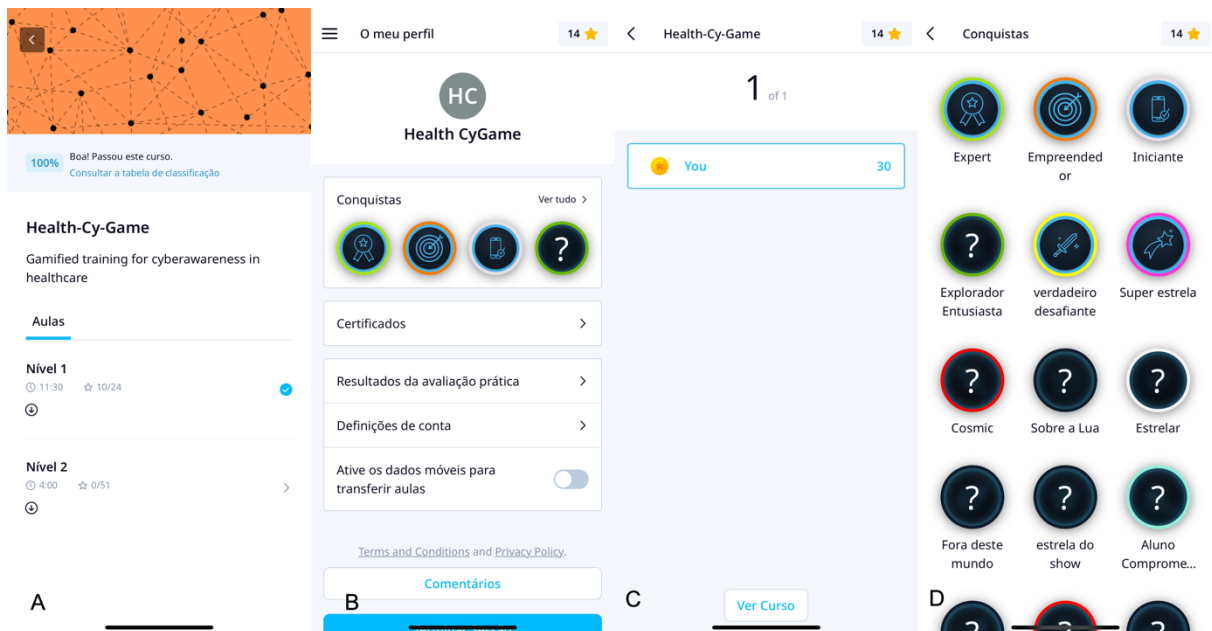


Fig. 4.4 – Health-Cy-Game: user’s perspective. A – Health-Cy-Game first screen; B – User profile; C – Leaderboard; D – Badges view

4.3 Lessons (Levels)

As stated before, the levels of the game will be represented by the term “lesson”, according to the terminology used by EdApp. The graphic design was personalized and created by the author. The logo (Fig. 4.2) was placed on the left corner of the screen and right next to it is possible to find the identification of the game level. Each level’s first screen looks the same (Fig. 4.5). The background changes between levels and was designed in four colors: purple, orange, green and salmon.



To best organize the levels and the game structure, the domains defined in section 3.1 will be grouped. In fact, while starting to design the game, it was possible to perceive that some domains, such as general knowledge on technology, include more extensive content than other domains, such as software maintenance and updating. To avoid creating a huge difference between levels and training topics, it was decided to group one more extensive domain with one that included less questions and topics to approach. Therefore, after making this link, the levels of the game and its related knowledge domains are:

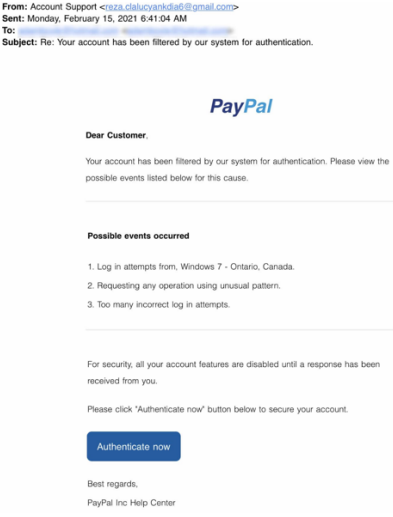
- Level 1: general knowledge of technology (computer basics and devices), software maintenance and updating.
- Level 2: data management, password management and authentication control.
- Level 3: cyberattacks most common techniques and how to mitigate their effects.
- Level 4: organizational procedures and requirements on cybersecurity.

Questions and short games were created based on the topics and domains defined (Table 4.2).

Health-Cy-Game is the prototype developed, as the prototype of the solution for gamified training of healthcare workers on cybersecurity. Organizational procedures and requirements on cybersecurity are a very important aspect, but it depends on the organization that it is being applied. Therefore, the prototype here presented, since it is not being developed for a particular institution, will include some sample questions for this domain, based on the reglementary documents published by Serviços Partilhados do Ministério da Saúde, E.P.E (SPMS), that reflect the general rules to all health institutions belonging to Portuguese national health system^{42,43}.

Table 4.2 – Exemplification of Health-Cy-Game’s questions and games

Game level	Topics	Games exemplification	Questions’ sample (answer)
LEVEL 1	General knowledge of technology (computer basics and devices), software maintenance and updating	“ <i>Quem quer ser tecnológico?</i> ” – multiple-choice format	<ul style="list-style-type: none"> • The mouse and the keyboard are examples of: (input peripheral components); • The size of a data set is expressed by: (bits, bytes, megabits and megabytes); • Keeping your computer up-to-date is important because: (updates protect against new risks and threats)
LEVEL 2	Data management, password management and authentication control.	Memory game: matching the attitudes of a fictional healthcare worker and the principles to achieve cybersecurity	<ul style="list-style-type: none"> • Rita went to have lunch. (She has ended her computer session and saved current work). • Rita's colleague has forgotten his access data. (Rita did not share her data with him.) • Rita took notes on a clinical file with another colleague's session. (Rita knows that, legally, the colleague assumes responsibility for the notes taken.)
LEVEL 3	Cyberattacks most common techniques and how to mitigate their effects.	“ <i>Que ataque sou eu?!</i> ” – matching between images and the type of attack related to the picture	 <p>Para continuar a usar o sistema, deverá pagar o resgate no valor de 1 milhão de euros!</p>  <p>- Ransomware</p>

		<p>“To phish or not to phish?” – classification of e-mails as phishing or real senders, with clarification of phishing techniques</p>	 <p>- Phishing</p>
<p>LEVEL 4</p>	<p>Organizational procedures and requirements on cybersecurity.</p>	<p>“Protect&Defend” game – multiple-choice format</p>	<ul style="list-style-type: none"> • You're at work when you receive an email that you're not sure is fraudulent, but you suspect it is. What you do? (Immediately delete the email); • If I need to install software on the organization's computer, I must: (Contact the IT department, indicating the software to the IT department and ask for its installation.)

1. First lesson (level 1)

- **Theoretical topics** - general knowledge of technology (computer basics and devices), software maintenance and updating.
- **Number of stars available** – 24;
- **Organization:**
 - a) Presentation of Cy and the goals of the training program (Fig. 4.6).
 - b) Presentation of basic topics and history facts about computers (launch date, creators and basic terminology about operating systems and components). One short game included (alphabet soup) about operating systems (Fig. 4.7).

c) Short-game “Quem quer ser... Tecnológico” (Fig. 4.8):

- 11 questions about computer science, basic concepts, software, and software updating.
- Multiple-choice format.
- Time limited (20 seconds per question).

d) Last game (jeopardy game) – “The ultimate challenge” (Fig. 4.9): the jeopardy game is a true or false game in which the questions are categorized by topics and distributed by different difficulty ratings. There’s a limit of time to answer each question. If the player answers correctly, wins more 4 seconds. If he does not, the game ends.

After the first level, if the player scores more than 75% of the total points possible, will have access to level 2. If not, the player will have to repeat the level after a 5-minute wait. The players will be ranked on a leaderboard according to their scores and will win badges as well. A user’s score is public, and every player will be able to see other players score on the leaderboard.

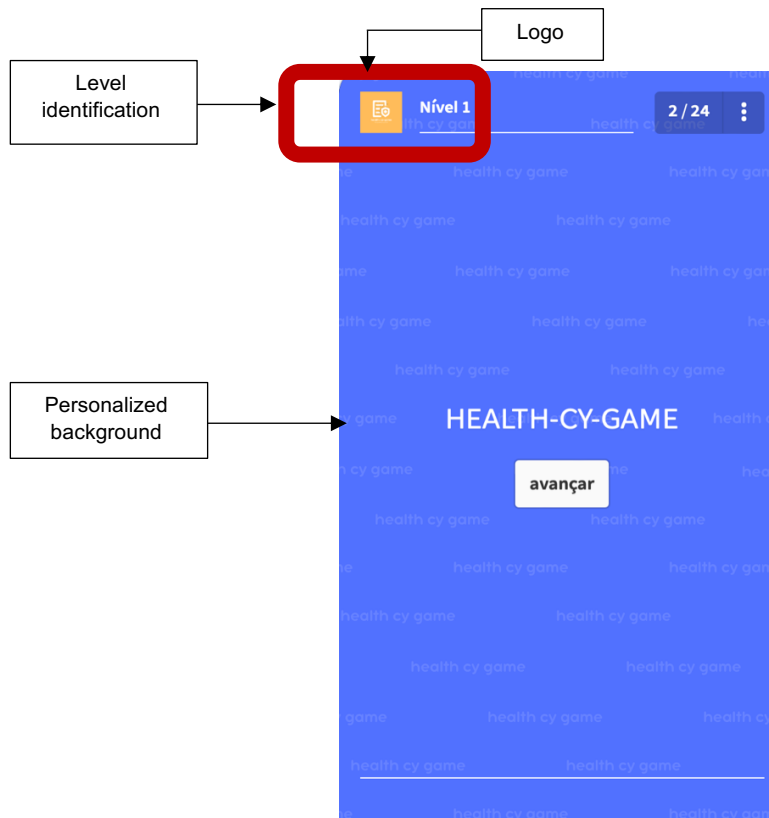


Fig. 4.5 – Health-Cy-Game first level home screen

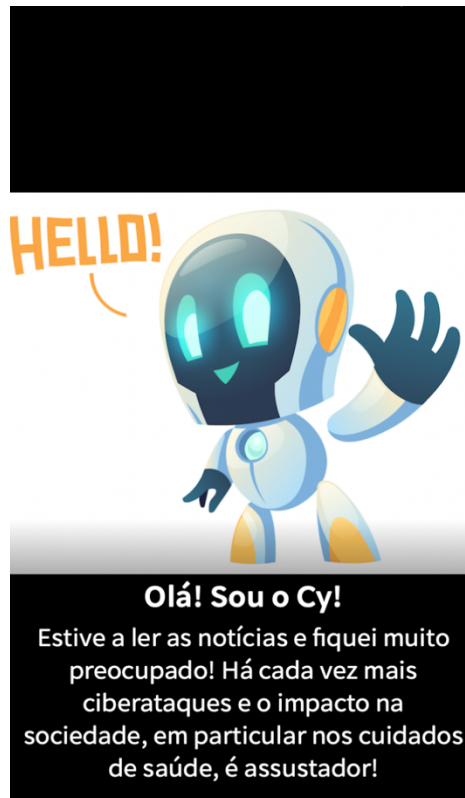


Fig. 4.6 – “Cy” (character) introduction

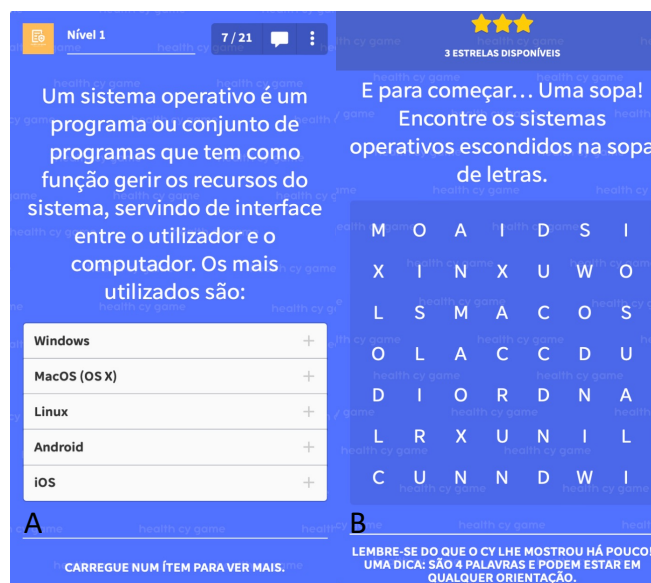


Fig. 4.7 – Exemplification of topics presentation (A) and “alphabet soup” game (B)

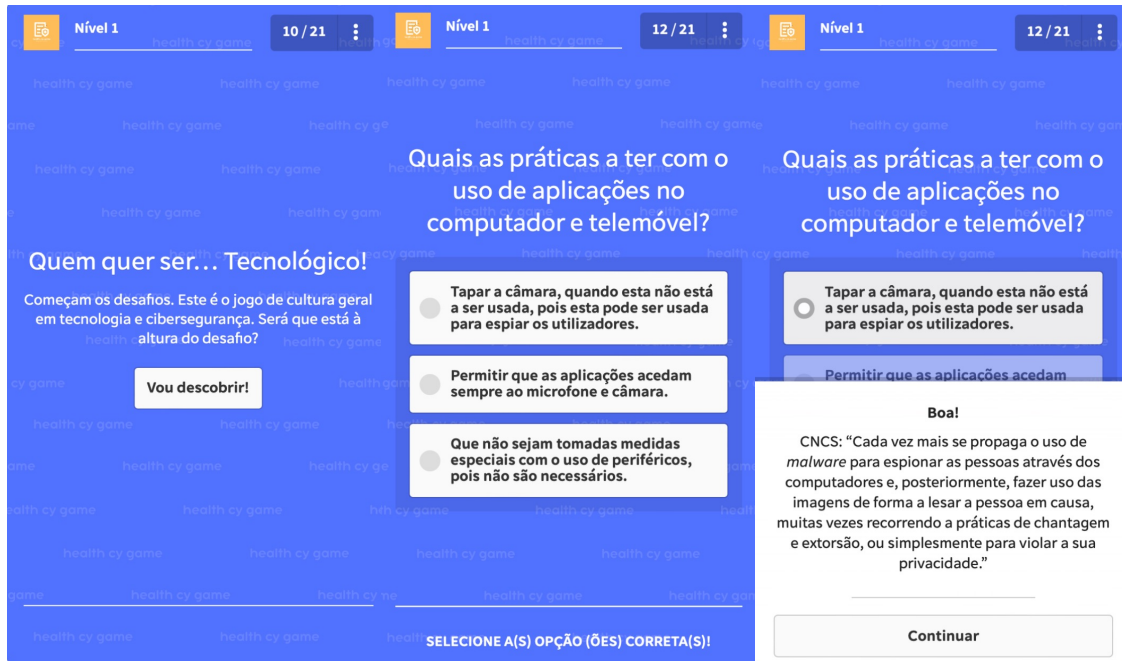


Fig. 4.8 - "Quem quer ser tecnológico" game template and question exemplification

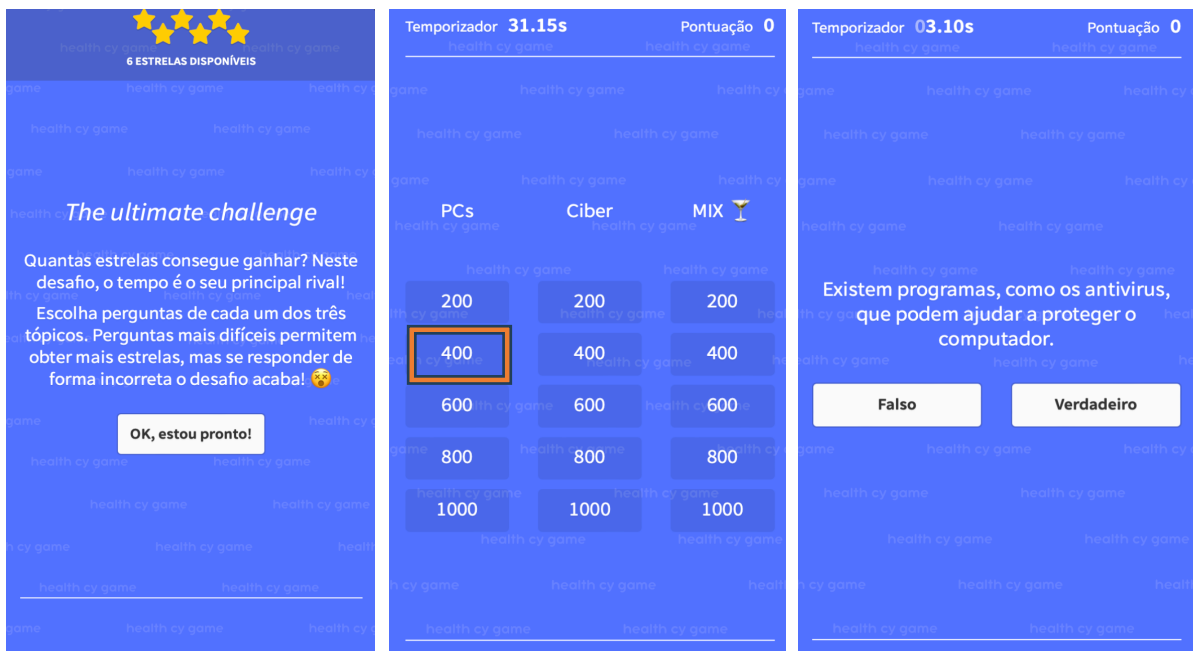


Fig. 4.9 - Jeopardy Game presentation. The showed question corresponds to punctuation 400 in "PCs" category.

2. Second lesson (level 2)

- **Theoretical topics** - data management, password management and authentication control.
- **Number of stars available** – 20;
- **Organization:**
 - a) Cy presentation of the topics included on the level (Fig. 4.10).
 - b) Series of short games that will allow the discover of basic concepts and actions by user itself (Fig. 4.11) All the games on this series will be time controlled, in order to increase difficulty.
 - c) **Last game (memory game) (Fig. 4.12):** in this game, the user will have to match the attitudes of Rita, a fictional character that represents a healthcare worker, and the correct actions to not compromise cybersecurity and safety of information.

After the second level, if the player scores more than 75% of the possible total points, will have access to level 3. If not, the player will have to repeat the level after a 5-minute wait. The players will be ranked on a leaderboard according to their scores and will win badges as well.



Fig. 4.10 – Cy presenting level 2



Fig. 4.11 – Exemplification of short-games used to present theoretical concepts



Fig. 4.12 – Last game: “Memory Game”

3. Third lesson (level 3)

- **Theoretical topics** - cyberattacks most common techniques and how to mitigate their effects.
- **Number of stars available** – 17
- **Organization:**
 - a) Cy presentation of the topics included on the level (Fig. 4.13).
 - b) Image map presenting the definition of the most common cyberattacks on healthcare sector (Fig. 4.14);
 - c) **Mini game “Alphabet Soup”** – to identify the techniques that can be adopted to protect a system;
 - d) **Short game “Que ataque sou?!” (Fig. 4.15)** – to match the image representing a cyberattack to the name of the cyberattack;
 - e) **Short game “To phish or not to phish?”** – to categorize the email presented as a real e-mail or phishing. In this game, after answering, the user can find a short explanation and tips to differentiate phishing from real e-mails (Fig. 4.16);
 - f) **Last game “The elevator game” (Fig. 4.17):** in this game, the user will have to match the attributes of each type of cyberattack on a popular game called “the elevator game”. Between each cyberattack technique, the user can find motivational phrases.

All the games will be timed controlled as well. After the third level, if the player scores more than 75% of the total points possible, will have access to level 4. If not, the player will have to repeat the level after a 5-minute wait. The players will be ranked on a leaderboard according to their scores and will win badges as well.



Fig. 4.13 – Cy presenting level 3

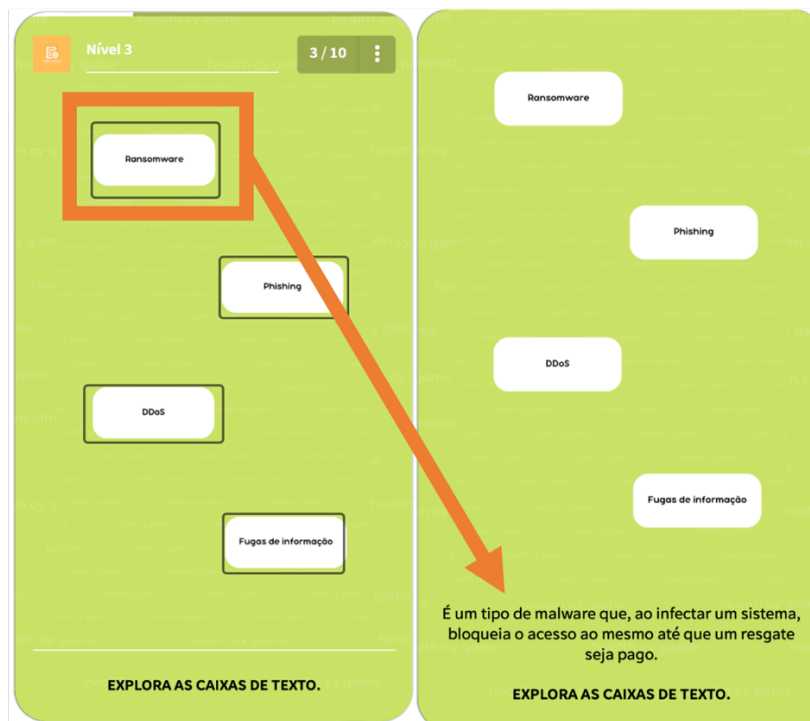


Fig. 4.14 – Image map containing the definition of the most common cyberattacks. When the user clicks on the box, the definition appears.

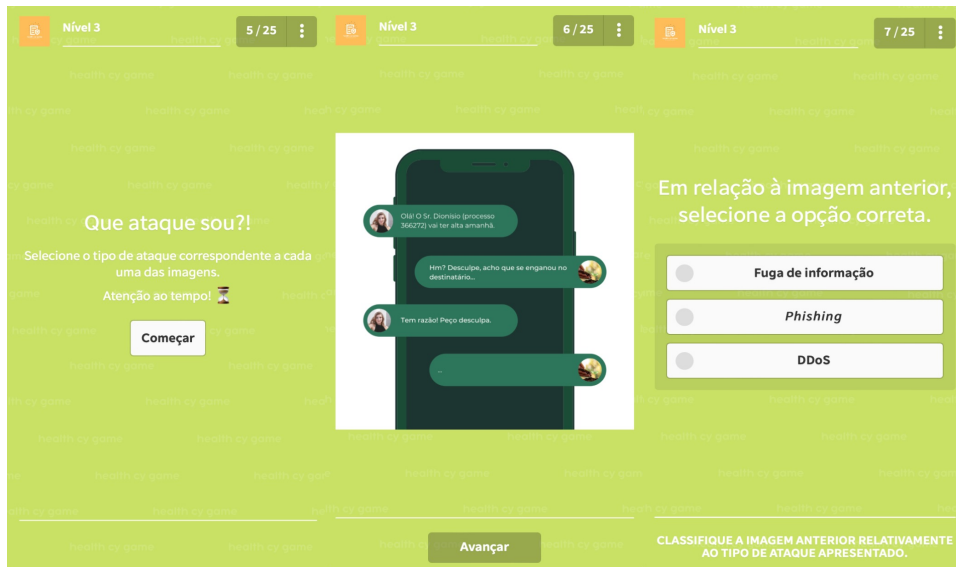


Fig. 4.15 – Short-game “Que ataque sou?!”

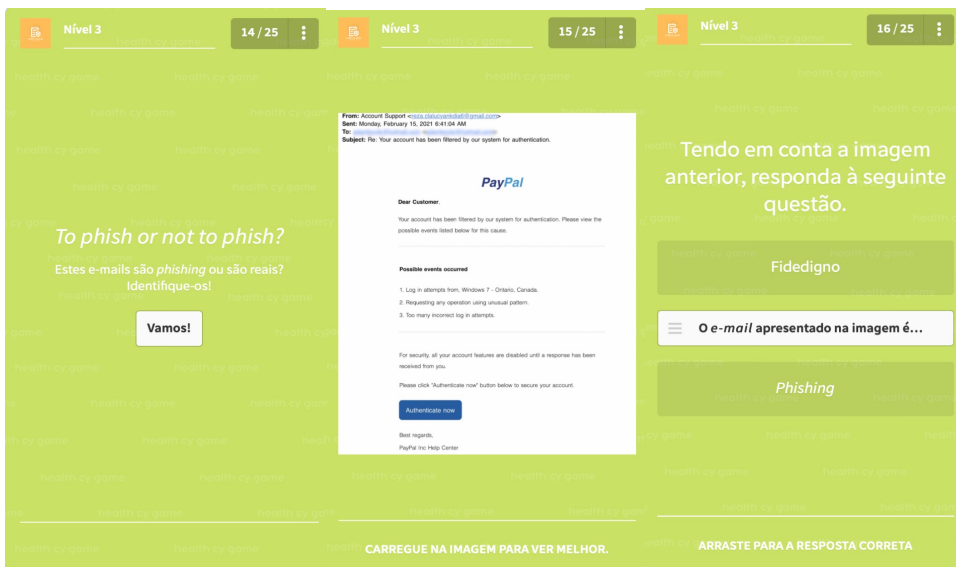


Fig. 4.16 – Short-game “To phish or not to phish?”



Fig. 4.17 – The elevator game

4. Fourth lesson (level 4)

- **Theoretical topics** - organizational procedures and requirements on cybersecurity.
- **Number of stars available** – 8 (level not completed)
- **Organization:**
 - a) Cy presentation of the level (Fig. 4.18).
 - b) Concept presentation regarding SPMS recommendations on cybersecurity (Fig. 4.19);
 - c) **Multiple-choice game “Protect&Defend”** (Fig. 4.20).

The theoretical concepts to be included on this level will depend on the specific procedures adopted by the institution on which the gamified training will be applied. Since the game is being developed to be used by Portuguese’s health institutions, the questions and topics presented were constructed based on the recommendations of SPMS. The level is not completed. More questions regarding the specific procedures to adopt in the case of a cyberattack will be added according to the recommendations of the health institution.



Fig. 4.18 – “Cy” presenting level 4



Fig. 4.19 – Theoretical topic presentation

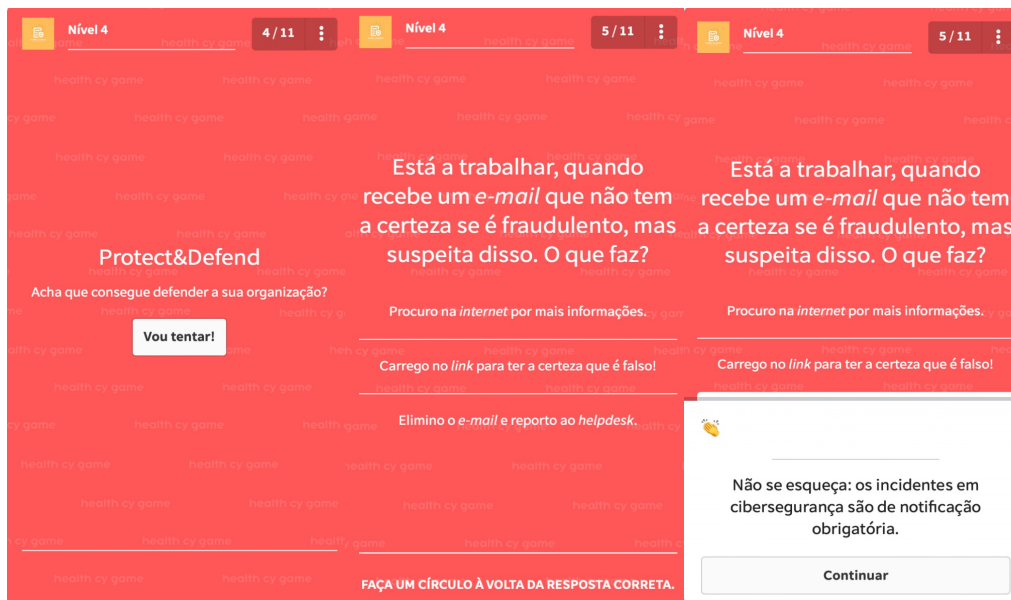


Fig. 4.20 – Exemplification of the multiple-choice questions of “Protect&Defend” game

5. Extra-challenge: HEALTH-CY-GAME QUIZZ

Rapid Refresh Quizz is a methodology developed by EdApp to increase learning retention. Once the users have finished Health-Cy-Game, the HEALTH-CY-GAME QUIZZ (Fig. 4.21) will be available, divided in three sessions.

To this challenge, a new leaderboard will be associated, and the users will receive notification via e-mail and push notifications to engage the quiz around 9 a.m. and the session will be available until the end of the day. The questions included are related to the learning topics of Health-Cy-Game. The points associated with this quiz are related to the number of questions correctly answered as well as the time the user took to do it. This means that if two players have the same score, the user who was faster to answer the quiz will be better classified than the other player.

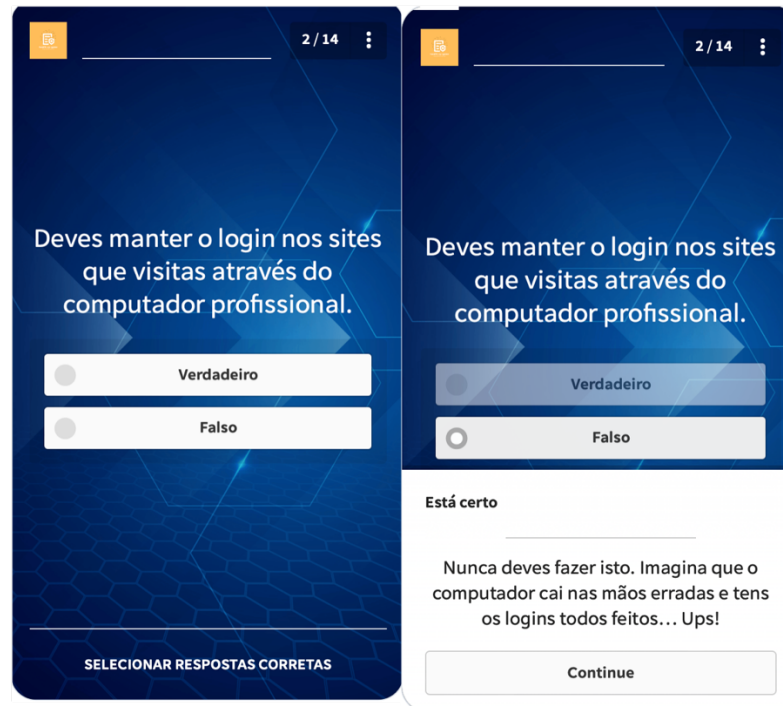


Fig. 4.21 – HEALTH-CY-GAME QUIZZ exemplification.
To each question, the justification of the correct answer will be presented.

6. Course certificate

Once the user completes the game, completing therefore the training program, will receive a course certificate (Fig. 4.22). The user's name, as well as the data of completion will be indicated.



Certificado de formação gamificada em cibersegurança

User's name

Certifica-se que [redacted] completou com sucesso a formação gamificada em cibersegurança, concluindo com distinção as tarefas do jogo **health-cy-game** a **Jan 22, 2023**



logo

making healthcare cyberaware

slogan

Fig. 4.22 – Course certificate

4.4 Octalysis framework applied to Health-Cy-Game



Fig. 4.23 – Health-Cy-Game: Octalysis Framework

As stated before, one of the tools used for assessment of gamification and its capability to influence human behavior is Octalysis framework²⁵. Applying its statements to Health-Cy-Game design (Fig. 4.23), and using the Octalysis tool developed by Yu-kai Chou (available from <https://yukaichou.com/octalysis-tool/>), the core drive with more score is accomplishment, followed by social influence and epic meaning, with empowerment, ownership and unpredictability occupying the same score. The core drive with less relevance is avoidance.

The gamification elements used related more with accomplishment core drive, representing the main goal of developing skills, progressing on the game and it is associated with the use of badges and leaderboards, along with a reward system based on points and scores. This is, in fact, aligned with the type of user defined on 6D framework: the player.

Social influence is achieved by the possibility to complete the game as a group, to participate on discussion forums to help other players to overcome the challenges as well as competition, resulting from the implementation of badges and leaderboards.

Epic meaning, the feeling that the player is important and belongs to something bigger, results from the implementation of the idea that this training is very important to make healthcare safe and empower them to make a difference.

Avoidance, on the other hand, is the core drive less explored on Health-Cy-Game. Avoidance relates to the need to avoid negative things from happening, being expressed by the need to act immediately to not feel that the opportunity was lost forever. Health-Cy-Game game's mechanics allow the user to retrieve a failed level after a 5-minute pause, not losing all the progress made on the other levels. User must redo all challenges of the level again, but since he does not lose the progress made so far, the urge to complete the challenge may not be present.

5 Conclusions

The present work aimed to develop a gamified strategy specifically designed for healthcare professionals. In fact, cybersecurity, due to its impact on health sector, should be integrated as a fundamental of data security and be a priority for health quality policies. However, to do so, it is important to leverage healthcare worker's cyberawareness levels and train them to this subject.

Health-Cy-Game is the prototype of the purposed gamified strategy. To design it, it was very important to identify the cybersecurity topics suitable for the purpose, keeping in mind healthcare workers profile, which is different from more specialized profiles like IT workers. It was explored national and international references and guidelines, such as CNCS' roadmap, SeBIS and RScB scale to select, according to relevant inputs, the domains that are suitable for healthcare workers profile related to IT usage and level of proficiency in cybersecurity. This is an important outcome of this project, since it may guide other authors on the development of solutions targeting health.

One of the main challenges of this work was the definition of the topics to include on the training session. There was not possible to find any recommendations targeting healthcare workers and its profile, differentiating by proficiency levels like there is, for example, to the engineering or management areas. This was an extensive and difficult work, which involved two major tasks: defining healthcare workers profile related to IT usage and the definition of cybersecurity domains to include on Health-Cy-Game.

Gamification needs to focus on the user type and defining appropriate gamification techniques and elements is mandatory to make it effective. The use of EdApp, an already validated and verified platform, eased the process of Health-Cy-Game's design. In fact, there was no need to focus on the coding and construction of the background, since it has all been integrated on EdApp. However, this also represented a limitation to the development of the strategy, since the choice of elements that could be applied and designed for the game were restricted to the ones included on EdApp. The creation of the game design was also a challenge. Developing a solution that was simple to use and understand while keeping it appealing and interesting was not easy, along with the integration of all the game elements and mechanics defined. The success of the gamified training is very dependent on its adequacy to its users, so the development of a general solution may not include all the users' profile and characteristics. The decision to go with the "player" type was, considering the goal of this dissertation, the most adequate since this is the profile in which most of the users fit, related to gamified elements that make gamification work: competition (with points and leaderboards) and motivation related to the feedback given using these elements.

While doing some research and benchmark of the existing solutions, it was not possible to find any designed specifically for healthcare and healthcare worker's profile. It is true that some available solutions, despite not being developed for this sector, could be applied to it, because of the training topics included, such as What.Hack or SpaceShelter, for instance. However, those games are designed for the public, free to access and were built to contribute to cyberawareness of general population. Health-Cy-Game development included the feedback from healthcare workers. Therefore, the situations presented are related to healthcare professionals' daily activities and challenges, aligned with their profile, being a more extensive training solution, incorporating all the domains defined for their profile. It was also developed in the Portuguese language, being more easily implemented on Portuguese health institutions, contrary to all solutions already existing that were developed in the English language.

Cyberattacks targeting health facilities are increasing. More recent literature defends that cybersecurity must be included in health institutions quality management programs, considering the major prejudice that comes for the patients and for the organization itself if a cyberattack occurs. Therefore, also keeping in mind that most attacks target users, raising cyberawareness is imperative. Providing cybersecurity training to employees is being considerate one of the requisites to guarantee cybersecurity¹⁹. Changing the fragilities of an institution will only be possible if all the stakeholders and members involved are considerate. There is no point in spending a significant amount on the most advance technology to protect a system, if then a user, not recognizing the threat, opens a phishing e-mail and runs the malware that comes with it. Investing in proper training of employees is fundamental to connect all the dots.

HTA is responsible for studying the effects of the technology associated with healthcare, focusing on its benefits and risks, measuring the direct and indirect consequences that come along with its use. Cyberspace is now an extension from the physical limits of health institutions. To study and to develop measures to minimize the direct and indirect consequences to institutions and patients associated with cyber threats is fundamental. If an error occurs that compromises patient safety, actions to minimize the chance from it to happen again are rapidly adopted. Cyberattacks may endangerer patient's life, or, at least, cause great disruption on the availability of care with huge impact on the workflow of national's health system. Therefore, efforts to make cyberattacks less probable or to minimize its impact must be taken, aligning strategies regarding technology development and innovation with cybersecurity policies on health institutions. Cybersecurity must be a concern for all the users of technology, despite their role and professional profile inside an institution, with, of course, proper adjustments on cybersecurity proficiency required based on the professional profile related to IT usage. Providing regular training on cybersecurity is essential and effective to

reduce cyberattacks. HTA stakeholders must also acknowledge training as a fundamental strategy to fight cybercrime, a simple action compared to more expensive and difficult ones, and incorporate training as a feasible solution against cyberattacks when developing procedures and guidelines regarding technology safety.

Health-Cy-Game was developed with the intend to make healthcare cyberaware, by providing proper cybersecurity's training to health professionals. With this project, it is intended to make health sector less vulnerable to cyberattacks, reducing its impact. We strongly believe that the next step, in order to verify the suitability of the developed strategy and its efficiency on cybersecurity training, would be implementing the solution at a healthcare facility, to a sample of healthcare workers. This thesis is a task of the project "Gamification Applied to Cybersecurity Education for Health Professionals" that it's being financed by IDI&CA, of Polytechnic Institute of Lisbon. The next step will exactly be the application of the strategy here developed to a sample of healthcare workers to perceive its efficacy. After testing it to a sample of healthcare workers and adjusting the developed prototype according to the feedback received, Health-Cy-Game will be ready to be implemented in a major scale to Portuguese health organizations. To do so, it would be important to create a designated work group to be working together with SPMS, dedicated to providing gamified cybersecurity training to health institutions, designing the training program. It would also be interesting to provide the training to all the healthcare professionals working in Portuguese institutions at the same time. This would promote social interaction between professionals from different organizations, using the discussion forum or completing the challenge as groups, and would be feasible because gamified training does not require a physical space, dedicated teachers and working schedules.

Gamification is undeniable changing education and training, being used in several domains with positive results. Healthcare sector faces new challenges related to worker's motivation and retention, especially in the public health sector. Introducing Health-Cy-Game as a cybersecurity training methodology, would not only contribute to the modernization of the sector, increasing worker's motivation and engagement, providing new experiences for employees, but would also contribute to raise cybersecurity awareness, mandatory to assure a safe technology improvement in health organizations.

6 References

1. McConomy BC, Leber DE. Cybersecurity in Healthcare. In: Clinical Informatics Study Guide. Cham: Springer International Publishing; 2022. p. 241–53.
2. 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(2):1–19.
3. Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*. 2018 Jul;113:48–52.
4. Onduto B, Doctoral P, Ali R, Smed AJ. Gamification of Cyber Security Awareness – A Systematic Review of Games. *Computing, Faculty of Technology*. 2021;(December).
5. WHO. Health technology assessment. https://www.who.int/health-topics/health-technology-assessment#tab=tab_1.
6. Ciberataques a organizações portuguesas aumentaram 81% em 2021 [Internet]. [cited 2023 Jan 3]. Available from: <https://www.itsecurity.pt/news/news/ciberataques-a-organizacoes-portuguesas-aumentaram-81-em-2021>
7. WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled | UK Healthcare News [Internet]. [cited 2023 Jan 3]. Available from: <https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled>
8. Collier R. NHS ransomware attack spreads worldwide. *CMAJ: Canadian Medical Association Journal* [Internet]. 2017 Jun 6 [cited 2023 Jan 3];189(22):E786. Available from: [/pmc/articles/PMC5461132/](https://pmc/articles/PMC5461132/)
9. The importance of cybersecurity in protecting patient safety | Cybersecurity | Center | AHA [Internet]. [cited 2023 Jan 3]. Available from: <https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety>
10. Kim J, Castelli DM. Effects of gamification on behavioral change in education: A meta-analysis. *Int J Environ Res Public Health*. 2021;18(7).
11. Boopathi K, Sreejith S, Bithin A. Learning cyber security through gamification. *Indian J Sci Technol*. 2015;8(7):642–9.
12. Kopetz H, Steiner W. Internet of Things. *Real-Time Systems* [Internet]. 2022 [cited 2023 Jan 4];325–41. Available from: https://link.springer.com/chapter/10.1007/978-3-031-11992-7_13
13. What is IoMT (Internet of Medical Things) or healthcare IoT? | Definition from TechTarget [Internet]. [cited 2023 Jan 4]. Available from: <https://www.techtarget.com/iotagenda/definition/IoMT-Internet-of-Medical-Things>
14. Ahmed MA, Sindi HF, Nour M. Cybersecurity in Hospitals: An Evaluation Model. *Journal of Cybersecurity and Privacy*. 2022 Oct 26;2(4):853–61.
15. 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(15):1–25.
16. ISO. ISO/IEC 27032:2012.
17. Cremer F, Sheehan B, Fortmann M, Kia AN, Mullins M, Murphy F, et al. Cyber risk and cybersecurity: a systematic review of data availability. Vol. 47, *Geneva Papers on Risk and Insurance: Issues and Practice*. Palgrave Macmillan UK; 2022. 698–736 p.
18. 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(7).

19. Triplett WJ. Addressing Human Factors in Cybersecurity Leadership. *Journal of Cybersecurity and Privacy*. 2022;2(3):573–86.
20. European Union Agency for Cybersecurity. List of top 15 threats - ENISA Threat Landscape. 2020.
21. European Union Agency for Cybersecurity. ENISA Threat Landscape Report 2018. 2019.
22. 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(November):1–13.
23. Queirós R, Pinto M. Gamificação aplicada às organizações e ao ensino. PACTOR. Lidel; 2022.
24. 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(7):1–20.
25. Chou YK. Yu-kai Chou: Gamification & Behavioral Design [Internet]. The Octalysis Framework for Gamification & Behavioral Design. [cited 2022 Sep 19]. Available from: <https://yukaichou.com/gamification-examples/octalysis-complete-gamification-framework/>
26. Moore M. Bringing Gamification to Cyber Security Awareness Training [Internet]. University of San Diego. [cited 2022 Aug 20]. Available from: <https://onlinedegrees.sandiego.edu/bringing-gamification-to-cyber-security-training/>
27. Adams M, Makramalla M. Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. *Technology Innovation Management Review*. 2015 Jan 29;5(1):5–14.
28. Nagarajan A, Allbeck JM, Sood A, Janssen TL. Exploring game design for cybersecurity training. *Proceedings - 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems, CYBER 2012*. 2012;256–62.
29. Nunes P, Antunes M, Silva C. Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions. *Procedia Comput Sci* [Internet]. 2021;181(2019):173–81. Available from: <https://doi.org/10.1016/j.procs.2021.01.118>
30. 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;(May).
31. Giannakas F, Kambourakis G, Gritzalis S. CyberAware: A mobile game-based app for cybersecurity education and awareness. *Proceedings of 2015 International Conference on Interactive Mobile Communication Technologies and Learning, IMCL 2015*. 2015;(May 2016):54–8.
32. CNCS - Referencial de Competências [Internet]. [cited 2022 Oct 30]. Available from: <https://www.cncs.gov.pt/pt/referencial-de-competencias/>
33. Egelman S, Peer E. Scaling the security wall : Developing a security behavior intentions scale (SeBIS). *Conference on Human Factors in Computing Systems - Proceedings*. 2015;2015-April:2873–82.
34. Hadlington L. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon* [Internet]. 2017;3(7):e00346. Available from: <http://dx.doi.org/10.1016/j.heliyon.2017.e00346>
35. Singapore Ministry of Health; Cyber Security Agency of Singapore. *Healthcare Cybersecurity Essentials*. Cyber Security Agency of Singapore. 2021;(August).
36. Tondello GF, Wehbe RR, Diamond L, Busch M, Marczewski A, Nacke LE. The Gamification User Types Hexad Scale. In: *Proceedings of the 2016 Annual Symposium on Computer-Human Interaction in Play*. New York, NY, USA: ACM; 2016. p. 229–43.

37. LeBlanc M. 8 Kinds of Fun [Internet]. Available from: <http://algorithmancy.8kindsoffun.com/>
38. Guion RM. Review of Managerial Behavior, Performance and Effectiveness. *Prof Psychol.* 1971;2(4):414–6.
39. Jun S jin, ChwaCheol S. Application and Effect Analysis of ARCS Model to Improve Learner’s Learning Motivation in Liberal Computational Thinking Subjects. 2020;24(2).
40. Hamzah WMAFW, Ali NH, Mohd Saman MY, Yusoff MH, Yacob A. Enhancement of the ARCS model for gamification of learning. *Proceedings - 2014 3rd International Conference on User Science and Engineering: Experience Engineer Engage, i-USER 2014.* 2015;(August 2017):287–91.
41. Feng SL, Tuan HL. Using ARCS Model to Promote 11th Graders’ Motivation and Achievement in Learning about Acids and Bases. *Int J Sci Math Educ.* 2005 Sep;3(3):463–84.
42. Serviços Partilhados do Ministério da Saúde EPE. Circular Normativa n.º 03/2017 - Medidas Excepcionais de Segurança [Internet]. Available from: <http://spms.min-saude.pt/alertas-e-seguranca/>
43. Serviços Partilhados do Ministério da Saúde EPE. Circular Informativa N.1 - Notificação obrigatória centralizada de incidentes de segurança (incluindo, entre outros, os de Cibersegurança). 2017 Feb.

7 Appendixes

7.1 Health-Cy-Game user's manual



TABLE OF CONTENTS

- 02**
what is health-cy-game
- 03**
getting started
- 04**
getting comfortable
- 05**
the ~~bo~~ing needed stuff
- 07**
reading your mind

WHAT IS HEALTH-CY-GAME

Health-Cy-Game is a gamified training strategy, designed for cybersecurity education of health professionals.

Health sector is an attractive target for cybercrime. Fighting this tendency is only possible with proper education and training of all the stake holders evolved. You are important to fight cybercrime!

Wait! Gami-what?!

Don't worry! Gamification means using videogame's elements to non-gaming situation, like training. This means to **have fun while learning!**

HEALTH-CY-GAME has been designed specifically for the health sector. Therefore, expect to find challenges and tasks that match your daily context!

Playing HEALTH-CY-GAME will allow you to explore several topics and domains on cybersecurity to improve your cyberawareness!

**"TELL ME AND I FORGET,
TEACH ME AND I MAY
REMEMBER, INVOLVE ME AND
I LEARN."**
BENJAMIN FRANKLIN



GETTING STARTED

1. Access your invitation e-mail

Congratulations! You are the chosen one!

Our team have sent you an e-mail with the information you need to get started! Read it carefully and follow the next steps.

2. Download and install EdApp mobile app



EdApp's mobile app is available for both Android and iOS systems. To download it, you can use the QR code on the left or find it at Apple Store or Google Play.

If you do not want to install it, you can simply go to web.edapp.com. But keep in mind that the experience will be better if you do!



3. Login using the details received on the e-mail

username: cyberawesomeisthenewthing

password: WoWo1234%\$

Trust me: complicated is the new safety guarantee!

4. COUNTDOWN: 3, 2, 1 - PLAY

Now it is time to sit back, relax, and enjoy the training program!

GETTING COMFORTABLE

The game is composed by four levels. The rules are simple.



SCORE TO PASS

You will need to score at least 75% to pass a level. If you do not make it, you have to retry the level after a 5-minute break!



COLLECT STARS AND SHINE!

Think of stars like the currency of the game. Stars will allow you to participate on the prize draws!



For each game, you have a set of stars that you can earn, depending on your performance. Do your best to shine!

BADGES

We want this experience to be one to remember! Because of that, your good discipline and dedication will be rewarded!



There's a diverse amount of badges that you can collect! But most important... These ones are not for your mother to exhibit on the living room.. They were created for you!

LEADERBOARD

Compete to spice things up! You will face your colleagues and you can check your position on the rank at any time!

5

THE ~~BOOKING~~ NEEDED STUFF

EXPLORING THE APP

How do you know you are killing it?!



LEADERBOARD

/li:da bɔ:d/
noun

1. a scoreboard showing the names and current scores of the leading competitors, especially in a golf match.

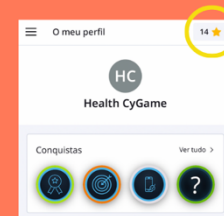
To check if you are the **alfa** of the game, follow these steps:

1. On the EdApp's mobile app homescreen, click on the menu side bar option;
2. Click on "Leaderboard";
3. Check your score!

Note: the leaderboard will represent the highest score you achieved! Imagine that you score 60 points on a lesson and retry it again, but score 100 points this time. Your score will be 100 and not 160. It is also the sum up of individual lessons' scores. If you score 80 on level 1 and 80 on level 2, your leaderboard score will be 160.

STARS

You can win stars by completing the challenges on each level as well as by logging in daily! We value your effort and will give you 2 stars per day!



From the starting page, you can see how many stars you own right next to the star icon!

BADGES

We want your profile to look good! But you have to deserve your style! 😊

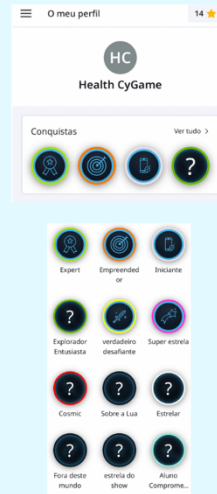
Badges will recognize your progress and there is a total of 17 that you can collect!

If your screen goes wild and something starts to pop up, be happy! You are doing great!

To check your badges, on your profile page, go to:

1. Achievements;
2. Click on "see all";

After this, you will be able to see all the badges you have already earned and the ones left to conquer, represented by an "?".



POINTS SYSTEM

All the lessons are scored to a maximum of 100%. To pass one level, you have to score at least 75%!

However, the **score** is not the same as the **points**.

The **points** are related to the challenges and games you have to face on each level. Having higher points will boost your lesson **scores**!

Also, **points** are used to collect **stars**. If you do not reach a certain number of points, you will not be able to collect the stars.



READING YOUR MIND

FREQUENTLY ASKED QUESTIONS

This is how a section like this is normally called.

1. HOW DO I ACCESS THE COURSE?

When you login on EdApp (using the mobile app or the online version) you will be able to locate HEALTH-CY-GAME right on. Click on it, select the first level and have fun!

2. HOW MANY LEVELS ARE THERE?

HEALTH-CY-GAME is composed by **four** different levels, each one corresponding to different topics on cybersecurity.

3. WHAT HAPPENS IF I LOGIN, BUT DO NOT PLAY?

That's sad! 😞 We hope you enjoy the game as much as we do! But to avoid that, you will receive push notifications (if permitted by you on installation) and e-mail notifications to remind you and motivate you to keep playing!

4. I DON'T LIKE MY SCORE! CAN I RETRY A LEVEL?

We really do like to see you motivated! You can retry a level hoping to get a better score as many times as you wish!

5. HOW CAN I SEE IF I WON ALL THE STARS?

In the lessons screen, right next to the lesson, there's a star symbol. You can see how many stars you have and the total of stars available on the level, represented by "10/24". This means you have 10 stars out of the 24 possible for that level.

6. MY COLLEAGUES ARE HAVING AN HARD TIME TO PASS A LEVEL. CAN I HELP THEM?

Yes, you can. If you or one of your mates are having an hard time to pass a challenge, you can use the discussion fórum to request for help and to discuss ideas. If this is not enough, the challenges can be completed as a group! The groups will be created accordingly to the feedback you give us and your engage on the discussion forum.

7. HOW MANY TIME DO I HAVE TO COMPLETE THE COURSE?

You will have three months to complete the course. This is more than enough!

8. WHAT SHOULD I DO IF I HAVE ANY OTHER QUESTION?

Our team is very happy to help you! Please reach us on heyitscgame@gmail.com and we will contact you shortly!



HEY, IT'S CY
GAME.



Gamification applied to cybersecurity awareness of health professionals, 2023

This project is financed by IDI&CA, IPL (project reference: IPL/2022/HeCyGame_ESTeSL).

Ana Carreiro | Carina Silva | Mário Antunes

7.2

Questions' database exemplification

	Question (answer)	Type of game	Difficulty
Level 1	Encontra os sistemas operativos escondidos na sopa de letras.	Letter soup	Yellow
	Qual/quais da(s) imagem (ns) correspondem a componentes periféricos de um computador?	Image correspondence	Green
	"Quem quer ser Tecnológico" Game		
	Um rato e um teclado são exemplos de... (dispositivos periféricos de entrada)	Multiple choice	Green
	O CNCs recomenda... (tapar a webcam, pois pode ser usada para espionar os utilizadores)	Multiple choice	Green
	O tamanho de um conjunto de dados é expresso por (bits, bytes, megabits e megabytes)	Multiple choice	Yellow
	À verificação composta por nome de utilizador e palavra-passe chama-se... (autenticação)	Multiple choice	Red
	Qual dos exemplos é um navegador (browser) de internet? (Firefox)	Multiple choice	Green
	Que nome se dá à pasta que guarda temporariamente os ficheiros eliminados? (Recicagem)	Multiple choice	Green
	Manter o computador atualizado é importante, porque... (as atualizações protegem contra novos riscos e ameaças)	Multiple choice	Yellow
	O "hardware" pode ser definido como: (Conjunto de componentes físicos de um computador, usados para introduzir informação, armazenamento, entre outros.)	Multiple choice	Yellow
	O "software" pode ser definido como: (Conjunto de instruções, data ou programas usados nos computadores e que servem para executar determinada tarefa.)	Multiple choice	Yellow
	Para garantir que o meu computador está atualizado, devo... (Permitir as atualizações quando for alertado para o efeito e não interferir com o processo.) + (Procurar a existência de atualizações, por exemplo, na janela do Windows Update.)	Multiple choice	Green
	Para uma correta gestão dos softwares do meu computador, devo: (Contactar o departamento de informática sobre problemas técnicos e necessidades adicionais para instalação.)	Multiple choice	Green
	Jeopardy Game		
	Category: PCs	True/False	Red
	Assegurar a cibersegurança é uma responsabilidade exclusiva do departamento de informática	True/False	
	Um computador é um dispositivo electrónico que recebe, armazena e processa uma grande quantidade de informação dependendo da sua programação.	True/False	
	O teclado, o rato e o monitor são considerados dispositivos periféricos de entrada.	True/False	
	Hardware é qualquer parte do computador com estrutura física.	True/False	
	Disco rígidos e pen drive são exemplos de dispositivos de armazenamento.	True/False	
	Google Chrome é um exemplo de um software de um computador.	True/False	
	Os computadores dividem-se apenas em dois tipos: desktop (computador fixo) e laptop (computador portátil)	True/False	
	Os tablets são exemplo de computadores portáteis.	True/False	
	Charles Babagge é considerado o pai dos computadores.	True/False	
	O computador Macintosh, produzido pela Apple, foi lançado em 1984.	True/False	
	ENIAC é o nome do primeiro computador e foi criado em fevereiro de 1946.	True/False	
	Category: Ciber	True/False	
	Confidencialidade e integridade são exemplos de princípios que não devem ser assegurados na cibersegurança.	True/False	
	A cibersegurança é, segundo a Microsoft, a capacidade de proteger recursos, informações digitais e dispositivos.	True/False	
A minha organização não precisa de se preocupar com cibersegurança, pois o sector da saúde não é um alvo atrativo.	True/False		
CNCs - Centro Nacional para a Cibersegurança - é a entidade máxima de Cibersegurança em Portugal.	True/False		

	Question (answer)	Type of game	Difficulty
Level 3	Encontra algumas das soluções que podem ser utilizadas para proteger um computador. (Firewall, antivirus and password)	alphabet soup	Yellow
	Que ataque sou?!		
	Imagem de Phishing - Phising	match game	Yellow
	Imagem de DDoS - DDoS	match game	
	Imagem de fuga de informação - Fuga de informação	match game	
	Imagem de ransomware - ransomware	match game	
	To phish or not to phis? Estes e-mails são phising ou são reais?		
	E-mail do PayPal - Phishing	categorize game	Yellow
	E-mail da EDP - Real	categorize game	
	Outro e-mail - Phishing	categorize game	
	E-mail com anexo - Phising	categorize game	
	Elevator game		
	Match between the cyberattack technique mentioned and its characteristics		
	Ransomware (exigência de um resgate para recuperação do acesso; impacto minimizado se as entidades fizerem backups recorrentes, bloqueio do acesso ao sistema após ter sido infetado por malware)	Elevator game	Red
	Phishing (associado a ataques ransomware, domínios do e-mail não coincidem com o nome da entidade, mensagens de carácter urgente).	elevator game	
DDoS (sistema sobrecarregado, afeta sistemas dependentes da internet)	elevator game		

7.3

Rapid Quizz question's database exemplification

	Question (required) - Suggested max 120 characters	Answer A (required) Suggested max 75 characters	Answer B (required) Suggested max 75 characters	Answer C (optional) Suggested max 75 characters	Answer D (optional) Suggested max 75 characters	Answer E (optional) Suggested max 75 characters	Answer F (optional) Suggested max 75 characters	Correct Answer(s) (required) Choose at least one	Follow up text to reinforce the answer (required) Suggested max 120 characters
Q1	Com quem deves partilhar as tuas palavras-passe?	Absolutamente ninguém!	Com o gestor de palavras-passe da minha equipa					A	A palavra-passe não deve ser partilhada com absolutamente ninguém!
Q2	Deves manter o login nos sites que visitas através do computador profissional.	Verdadeiro	Falso					B	Nunca deves fazer isto. Imagina que o computador cai nas mãos erradas e tens os logins todos feitos... Ups!
Q3	Qual é o principal objetivo de um hacker ao realizar um ciberataque?	Perturbar o normal funcionamento de uma organização	Espalhar informação útil	Lucrar financeiramente com a operação				A, C	Os ciberataques têm um impacto económico bastante relevante para as organizações!
Q4	Como pode um malware afectar a rede da organização?	Se não desligares o computador corretamente	Se carregares num link suspeito e instalares software desconhecido	Ao usar um computador durante várias horas.				B	O malware (ou software malicioso) é usado para enfraquecer um sistema e pode infectar a rede da organização através de links ou da instalação indevida de software.
Q5	Não há problema em ignorar notificações sobre updates e segurança.	Falso	Verdadeiro					A	Manter o software atualizado é fundamental para garantir a segurança!
Q6	Como atua a firewall para proteção de acessos indevidos ao computador?	Notifica as entidades governamentais da presença de software infetado e identifica seus criadores (hackers)	A firewall fiscaliza toda a informação que passa pelo computador e identifica as ameaças presentes.					B	A firewall tem como função rastrear toda a informação que entra e sai de um computador, com o objetivo de identificar e neutralizar ameaças!
Q7	Deves abrir ficheiros anexados a mensagens de remetentes desconhecidos?	Não!	Sim! Não há problema. O antivírus protege-me.					A	Os softwares de proteção não são 100% eficazes contra o malware. A proatividade é fundamental na cibersegurança!
Q8	O que deves fazer se receberes e-mails de remetentes desconhecidos?	Enviar o e-mail para o meu chefe.	Abrir o e-mail e anexos para confirmar a fonte.	Bloquear o remetente e apagar o e-mail.				C	Apagar mensagens de remetentes desconhecidos e NUNCA abrir os ficheiros anexos é imperativo! O phishing é uma das técnicas usadas para propagar malware associado, por exemplo, ao ransomware.
Q9	Qual o aspecto de e-mails de phishing?	Parecem de fontes confiáveis.	Mensagens com um carácter urgente.	Às vezes, estão associados a ofertas e prémios.				A, B, C	Os e-mails de phishing parecem de fontes confiáveis e entidades respeitadas e conhecidas. Estar atento ao domínio do e-mail, à forma como a mensagem está escrita e verificar se existem ficheiros anexos são etapas fundamentais para os reconhecer.
Q10	Qual dos seguintes te pode ajudar a evitar e-mails de phishing?	Usar o e-mail só no meu computador pessoal.	Verificar o e-mail com regularidade.	Definir os filtros de spam para o nível mais elevado.				C	Todos os sistemas de e-mail têm filtros de spam. Para ajuda na sua configuração, contacta o departamento de informática da tua instituição!
Q11	A informação sensível de uma organização só pode ser roubada dentro da organização.	Verdadeiro	Falso					B	A informação contida, por exemplo, nos computadores portáteis e telemóveis da organização também podem ser alvo dos hackers e comprometida fora dos limites da organização.
Q12	Se tiver dúvidas quanto à possibilidade de estar a ser vítima de um ciberataque, devo:	Contactar imediatamente o departamento de informática da instituição.	Ignorar. Certamente que o sistema sabe como reagir.	Mandar mensagem ao meu chefe.				A	Mitigar os efeitos de um ciberataque depende do tempo que decorre entre os primeiros sinais e a sua identificação. Todos podemos ajudar!
Q13	Garantir a cibersegurança na minha organização é uma responsabilidade exclusiva do departamento de informática.	Verdadeiro	Falso					B	Todos os profissionais são actores fundamentais na garantia da cibersegurança.
Q14	Para repor a normalidade com mais rapidez, a minha organização deve fazer backups regulares da informação.	Verdadeiro	Falso					A	A DGS recomenda que as organizações mantenham backups regulares da informação crítica e mantenham esses backups seguros.