POLITECNICO DI TORINO
Corso di Laurea in Computer Engineering

Master Thesis

Gamification for Improving Cybersecurity

Advisors
Prof. Antonio Lioy
Prof. Andrea Atzeni

Candidate
Chiara Oggeri Breda

Academic Year 2021-2022

Summary

This thesis explores gamification and its application to cybersecurity. It is well known that nowadays the weak link in cybersecurity are humans. On one hand, both for personal and work businesses the connection and the use of devices are needed also for not computer science and cybersecurity experts. On the other, the lack of professional figures in the cybersecurity market with precise skills increases the need to train new experts in the field. For these reasons, concentrating the attention on the end users, with the purpose to create a useful education and awareness is important and the thesis proposes gamification as a possible solution.

The work starts to analyse gamification in general with its theories and frameworks. Gamification uses, in a non-gaming environment, game components and mechanics that involve and engage human attention encouraging a change of behaviour. I started to analyse gamification frameworks and theories to present as fully as possible the mechanics that are the basis of gamification and how it is used to encourage users in actions that are usually considered unpleasant. Most frameworks presented underline the motivators, user journey, rewarding system and in general guidance on the development part of experiences with gamification.

After a general presentation, the work focuses on cybersecurity fields. The work starts to analyse why the use of gamification in this specific field can bring satisfactory results. Therefore, the work starts with literature review. The key elements analysed that gamification should be offered are: immersive learning, increase participation, engagement and change of behaviours. Gamification is presented as a possible solution to counterbalance the limits of the standard training and awareness programs and general education in cybersecurity.

The work analyses the state of the art, distinguish three areas of interest: work, education and private environment. The aim to analyse the already developed gamification experience only in cybersecurity fields is to collect choices and development techniques, results and limits concerning the different environments. The literature does not present frameworks related to the application of gamification in cybersecurity, however, it is possible to analyse frameworks related to serious games about cybersecurity. Although serious games are not the focus of the work, their analysis is useful for the thesis purposes to underline methodology, guidance and topics directly linked with security. The key issues presented underline methodology and development choices not yet precise, privacy limitation and ethical problems.

The work has continued with the aim of retrieving information from different sources with different backgrounds:

- End-users, in general, not cybersecurity experts. We submit a survey to collect cybersecurity perception, knowledge and feelings referred to the cybersecurity awareness program already followed. At the same time are collected ideas and considerations to the application of possible future awareness programs in the work environment with gamification.

- Gamification experts, thanks to Francesco Lutrario, it was possible to collect interesting information, suggestion and elements to avoid related to the application of gamification in a work environment. With interaction with the ProjectFun Italian community, it was possible to interact with experts and enthusiasts in gamification in order to collect opinions and suggestions on possible applications and methodology.
- Cybersecurity experts with experience in gamification applications. Yanick Fratantonio shared with us his experience with a university course on mobile security organized with gamification elements.
- Observations obtained by professors that try to apply active learning in their lectures and share their experiences during conferences to improve teaching techniques.

The combination of the knowledge obtained through literature reviews on basic gamification theories and framework, framework referring to serious games in cybersecurity and the information obtained through comparisons with users and experts are summarized in order to define a methodology focused on gamification in cybersecurity context. The methodology focuses on cybersecurity skills, tools, rules, gamification elements, elements of influence, elements to avoid, purposes of usage, fruition time and support instrument during the development phase.

As support to the methodology developed some solutions are analysed:

- A future possible application mainly based on cooperation as a game element in a technical context as master of science degree in cybersecurity. The idea is based on a long term program during both the years of Master of Science graduate program provided by Politecnico di Torino with different experiences as integration of standard lectures. The use of game experience has its aim the practical application of concepts learned during the standard lecture and to create a critical thought about cybersecurity topics, with continuous learning. The work tries to analyse a possible implementation keeping in account some possible issues and proposing solutions.
- As a case of study, a computer security program with several elements of gamification provided by the platform TryHackMe during the advent period in relation to the methodology proposed.

To conclude the work, we provide some possible applications following the methodology created previously: in the context of a course provided in Politecnico di Torino, it was organized a little experience focusing on certification authority.

In future work, it will be possible to practically implement a gamified experience starting from the proposed project, in order to improve the methodology by defining limits and strengths thanks to practical feedback. Moreover, it will look for gamification experiences in the workplace, trying to gather experiences and ideas from companies that already use them. In fact, for future extensions, it will be interesting to collect more information and apply the methodology from the working environment.

In particular, my work has been to collect extensive information about gamification and frameworks in the field of interest. I have scientifically analysed the advantages and limitations of literature and researched new sources and direct experiences. The data collected and analysed were summarized in a new methodology that allows its use both as a support in the implementation of gamification experiences and the analysis of existing activities. The work done included problem definition, synthesis of strengths in an original methodology, development and implementation of analysis on the present situation.

Acknowledgements

First of all, I would express my gratitude to Professors Antonio Lioy and Andrea Atzeni for allowing me to explore this interesting and current topic and for actively assisting and supporting me through my thesis work.

I would like to thank all the experts who have dedicated their time to share their knowledge and ideas about the project. In particular Professors Francesco Lutrario, Yanick Fratantonio, and the ProjectFun community.

I would also thank all the Politecnico di Torino Professors involved in the organization of the "Teaching week" in particular thanks to Professors Fulvio Corno and Cristiana Rossignolo for allowing me to participate and gather valuable information and testimonials for my work.

A special thank goes to all the survey participants both end-user side and "Project Work" students, their interaction has been fundamental for a coherent work that takes into account and focuses on the end-user.

I thank my whole family, in particular, my mother Monica, my father Marco and my sister Lucia. They have always placed trust in me and supported me in all my choices during these years. I would also thank my grandfather Renato, my aunt Lea and my cousins Marta and Erica, they have always been there for me.

An infinite thank goes to Alberto. I thank him for his presence, perseverance and patience. He always gives me the best moments of light-heartedness. I thank him for encouraging me to believe in me during every little failure and for celebrating with me every little achievement.

I would express my gratitude to Anna and her amazing family with Stella and Danilo. She is my strong point of reference. Thanks to her for always being available to challenge and advise me in any situation.

Contents

Chapter 1

Introduction

1.1 Context of Analysis

In recent years, technologies relating to cyber security issues have become more precise and ensuring an increased level of safety. However, humans are often the weak link and for that reason they represent the principal vulnerability for many attacks. It is well known that nowadays the number of attacks is increased especially for phishing, social engineering and malware. Definitely because of the pandemic remote working is increasingly common [1]. Therefore, correct information and training in security fields are necessary to protect users and companies from vulnerabilities.

About 90% of computer security violations are caused by human errors, as reported [2] less than 1% of the attacks are made by the use of system vulnerability the rest exploit the human factor This problem is caused both for very little awareness by people in general not experts in security and by the massive use of attacks that include social engineering elements. The idea that only experts in security know how to defend themselves about to cyber security is wrong, especially in a world that every day is connected to the internet and devices. The most used types of attacks are phishing and other forms of social engineering and ransomware. In 96% of the cases, phishing is delivered by email, rarely by malicious websites or phones. However, it is used often as a first infection vector, with the purpose to infect the target as the source for other types of attacks [3].

A survey reports that 64% of Americans do not know how to control if they were affected by a data breach and most of them do not know what to do if they were under attack [4]. This data report is a big problem in a society data every day is connected. Another crucial element is the security of the smartphone: the user perception about cyber security related to the smartphone seems to be much less than the attention used for PC [5]. At the same time, also the application downloaded on the devices can be malicious, but in general, people keep less attention to the phone. The increased use of mobile apps and the increased number of available applications that enable new functionality at the same time open the door for new risks for the user. The number of malwares on mobile platforms increase rapidly by about 125% between 2011 to 2018. In 2019 24000 malicious mobile apps are detected every day [5]. This cognitive bias is a problem for personal and company security: increasingly the smartphone is used as the main support for both personal and work business. The type of attacks is modified in order to exploit these errors of perception. For example, a variation of phishing attacks is smishing. It is the replacement of emails with messages, always intending to induce users to provide personal information and then be able to implement any attacks. There exist a lot of variation of the standard phishing, but this specific technique is used become it seems that users have a much lower perception of risk when they are using smartphone [6].

The difficulty in acting does not only affect individual citizens but more, in general, the company [7]. In media, attacks take 280 days to be recognized and two-thirds of global business leaders would have difficulty responding to a cyberattack, especially due to a lack of internal skills. This element underlines also the lack of competent security personnel concerning the request.

The human factor is not only a problem for private citizens but also companies. For example, in 2018 the top industries targeted were finance, manufacturing, technology, healthcare, retail, construction, automotive, IT and education [2]. Another relevant element to keep in consideration is the security for the small and medium-sized enterprises. It is natural thinking that small and medium-sized enterprises have few risks about cyber security, but obviously, this is not true. Both for the natural digital transition and the use of information systems, which also include small farms and for the evolution of cybercrime attention to cyber security is needed. The most present type of attack used against companies is ransomware: the attacker blocks the target system and asks for a ransom. A version of this attack is the data theft and the public exposition of the data, this creates damage for both data loss and for companies' reputation. According to [10] in small businesses (with less than 500 employees) in 2021 the data breach costs is increased from $2.35 million to $2.98 million with a 26.8% increase. This element underlines the necessity also for small enterprises to create a strong cyber security culture. With the pandemic and the work from home, these problems have been freed, often companies did not have a cyber security plan to transfer the remote work and rarely employees are formed in a small and medium-size company to protect themselves and the work for cyber-attacks and vulnerabilities [8].

The main consequences that it can run because of an attack are losing data, privacy, intellectual property and money [9]. Most of cyber-attacks are financially motivated, then theft of intellectual property and espionage. It is also important considering the cost associated with cybercrimes. According to [10] the cost of data breach increase year over year by about 10%, in 2020-2021 the data breach costs amount to $4.24 million. The average cost is $1.07 million higher in breaches where remote work was the cause. Another interesting data is the lost business caused by a breach of system availability and diminished reputation. The personally identifiable information is the costliest record type with $180 per record. The compromised credential is the most common initial attack vector, with its use in 20% of the breaches both in business environments and in private ones.

For all these reasons it seems clear that education in cybersecurity is needed to increase the users' awareness, especially to raise awareness of all those attacks that as the main target have humans. On the other hand, it seems necessary education for cybersecurity experts, and incentive young students to study cybersecurity topics to close the gap between the demand for specialized figures and the actual ability of the workers. Some recent reports figure out that often companies do not invest enough in training and awareness. In 2018 only 45% of companies provide a mandatory course about cyber security: only 10% follow a frequent update (monthly or quarterly) and about 10% take a course only once in the recruitment phase. Another important topic is how this knowledge is provided: about 33% of the companies offer employees emails with lists that describe suggested behaviours. It is clear that this approach usually risks being ignored [11].

As reported [12], when used, the standard security awareness and training program often fails its work. The main problems reported are:

- Engagement: these courses have as principal aim to increase awareness and consequentially change behaviour in users. However, often the user feels the course is a corporate obligation, so complete the task but without a real interest and attention. In the end, the result is that the theoretical knowledge is acquired but in practice, the behaviour does not change. Involve the user in topics is important to increase awareness and outcome in the change of behaviours.

- Personalization and no plan: they are important to organize the awareness program with a plan considering goals, topics, how to communicate, target and user work role. Often the standard education is equal for everyone without keeping into consideration previous knowledge or interest and the role held within the company. In this way is extremely hard to create a real education and interest in the users. This could cause insecurity in users that reflects on the company security and result.

- Learning update frequency: for education and security awareness it cannot be organized in singular or sporadic events. Usually, companies organize an annual or twice a year refresher training for their employees. However, it is not enough to face the new attack techniques

and create a strong change of behaviours in users. It was necessary for continuous and specific education in a long term life cycle.

1.2 Gamification

The term "Gamification" has become popular since 2010 and its definition is the use of game elements, mechanics and dynamics in a non-gaming context. The aim of gamification is the improvement of the perception of the context in which it is applied that comes with increased motivation, involvement, change of behaviours and habits, support for memorization and difficulties and limits reduction.

This technique should be applied in many different contexts as Education, Fitness, Entertainment, Advertising, Healthy. Some examples are reported here:

- In the fitness sector an example of gamification is "Zombies, run!". It is a mobile application used to track the running session. When the user starts to run, thanks to a story that the user can listen to, he is encouraged to escape from zombies, complete missions and find objects. In this case, the use of game elements has to purpose to create progress and improvement in fitness activity [13].
- Also, in the marketing sector the gamification is often used, an example is SNEAKRS an application dedicated to a portion of Nike customers. The users can access limited editions of shoes only if they found some elements inside the app, use geo-localization in specific physics points and complete the missions propose. In this example users are motivated thanks game elements to interact with the application and obtain shoes [14].
- Considering the educational sector Duolingo is one of the greatest examples of gamification. It is an application with the purpose to learn new languages. Inside the application are used some game mechanics and dynamics to learn the selected language. User is encouraged to follow short lesson once a day thanks to the game elements like progress bars, badges, points, leader-boards and tests [15].
- In the Healthy environment a significant example is reported thanks to the Presbyterian Morgan Stanley in New York. The hospital room dedicated to the paediatric CT scan is transformed into a ship of pirates. In this way, children are helped and encouraged in dealing with fear, stress and anxiety during hospital stay thanks to storytelling [16].

Therefore, gamification intend to accompany the user in difficult and tiring actions for several reasons reducing mental effort thanks to the help of game elements.

This gamification concept is based on different psychological, communication theories and cognitive biases. Some of the most important related theories are:

- Flow Theory
- Self-Determination Theory
- Gamification Learning Theory
- Fogg Theory
- Bloom Theory

There are different frameworks already developed that try to theorize various aspects of this subject:

- Octalysis
- MDA

- GAME
- 6Ds
- EEEE
- User Types Hexad
- Gamification Canvas Model

The most relevant aspect to take into consideration is the analysis of **users' type**, what motivates people and the relation between different mechanics and dynamics among user behaviours.

Different studies report the efficacy of gamification in terms of change of behaviours, engagement and long-term motivation. Some studies analyse the different game design elements and their applicability in different contexts, the most popular are:

- Challenges appropriated to the target
- Leader-boards (Points, Ranking)
- Progress Bars
- Game Fiction
- Collaboration and Competition
- Narration

Another gamification feature is that for definition there may exist some form of **metric** or control to determine in perfect way progress and results. This element makes comparison a default element necessary to measure real effects and make it possible to take a decision on actual data. Each context needs specific metrics also because the purpose of each project and the data sources can be extremely different.

1.3 Gamification for cybersecurity

Some companies, understanding the inefficient of standard training and awareness model, try to change it and start to experiment with gamification strategy. What was found is that the standard education can be compared with a not education at all. Standard education in the cyber security field is intended as email, passive education (reading, listening), mandatory courses.

The gamification process includes the complete or partial immersion of the user in what he is doing. This immersion helps the memorization process and the change of behaviour. However, it is needed a constant and a lengthy period of interaction with the system in order to appreciate the results. The literature does not present a standard methodology or implementation and a fixed mode to choose game elements to insert. Anyway, all the companies that experiment with this method have found benefits in the number of attacks incurred, the number of reports received by the security department of suspicious elements and the number of hours saved in repair and in training needed.

The gamification technique uses dynamics, mechanics and contexts typically of the game world in a not gaming environment with the aim to incentive and motivate people to do actions normally considered heavy and boring. Gamification and its application in the cybersecurity context have the goal to increase attention, motivation and knowledge also for not expert users in order to limit the risk of exposure. Interaction and involvement should be a great starting point to engage and motivate users to a safer and more conscious behaviour in order to protect themself and their companies [17]. This technique puts at the centre of attention humans, before technologies, and it tries to close the gap between what "we have to do" rather than what "we want to do".

The use of gamification in cybersecurity has also the aim to increase practical knowledge, one of the main game features is that it is necessary to practice. This element is well-linked

with cybersecurity because it is a subject that needs action and needs user acts recognition of dangerous situations [18]. Moreover, the use of game-like situations can include new targets to approach cybersecurity both for awareness and for work purposes. Live the training as a game during with is allowed make mistakes, ask for help and create relationships with peers in a relaxed and fun environment can improve the knowledge acquired.

Some gamification examples in cybersecurity are reported here, these references are better analysed in chapter 3:

- In a work environment was created a web application to educate employees about phishing attacks. During the experience were present clear objects, immediate and not ambiguous feedback and a correct balance between challenge and users' skills. As game elements were used avatar, scoreboard, points and feedback. This experiment was carried out to compare results between standard education, via email, and gamification thanks to a real phishing simulation. The result report that gamified education increases by almost double user perception and awareness [19].
- In the education environment an example is represented by [20]. Standard university lectures were supported also by a gamified platform. Students were free to choose if use or not the gamified platform, the final grade does not consider their participation. As most crucial elements of gamification used were storytelling and metaphor to introduce the cybersecurity technique aspect. The final result report that users that chose to use the support platform increased their final grade compared to students that only followed the standard lectures.
- Other forms of gamification in cybersecurity are free to use also in private spaces. Space Shelter represent an interesting example [21]. It is a short game created by Google and Euroconsumers with the purpose to increase awareness in normal users. Some game elements used are challenges and tests, avatar, storytelling.

For these reasons, there are bases to believe that gamification can give positive results in cybersecurity fields.

Chapter 2

Background

2.1 Theories Related to Gamification

Gamification, in general, finds its basis in different theoretical concepts related to psychology, communication elements, learning strategy, brain habits and cognitive biases. These theories explain why gamification can work by exploiting humans' behavioural characteristics. It is also theorized which kind of motivators work for our brain. In order to understand the gamification structure, implementation and framework it is needed a little background in theories that support gamification.

2.1.1 Flow Theory

The Flow Theory, theorized in 1997 by Mihaly Csikszentmihalyi, explains the experience in which the human is completely focused on the task assigned because of total involvement. People in flow lose awareness of the world that surrounds them: other people, distractions, track of time [22]. This theory is based on the correct choice of the challenging task level in correlation with the individual skills on that specific task. As shown in figure 2.1 distinct levels of challenge difficult in relationship with the specific skills can induce the user in different emotions: apathy/boring (low skill, low challenge), anxiety (low skill, high challenge) and flow (high skill, high challenge).

Factors that can lead to an experience of flow are:

- Clear goal
- Immediate feedback
- Total concentration on the task
- Distortion of temporal perception
- Correct balance between challenge and skill
- Intrinsic motivation
- Sense of control

The Flow theory is at the base of each game and can be used also in gamification. Flow can be seen as a channel between anxiety and boredom and should represent the "Player Journey", which takes users from beginning to end with the correct increasing level of challenge as soon as the user learns new skills and competencies. The ideal path provides the increase of difficulty after each "boss battle" applied as a test for the users from on-boarding to mastery level, as shown in the figure 2.2.

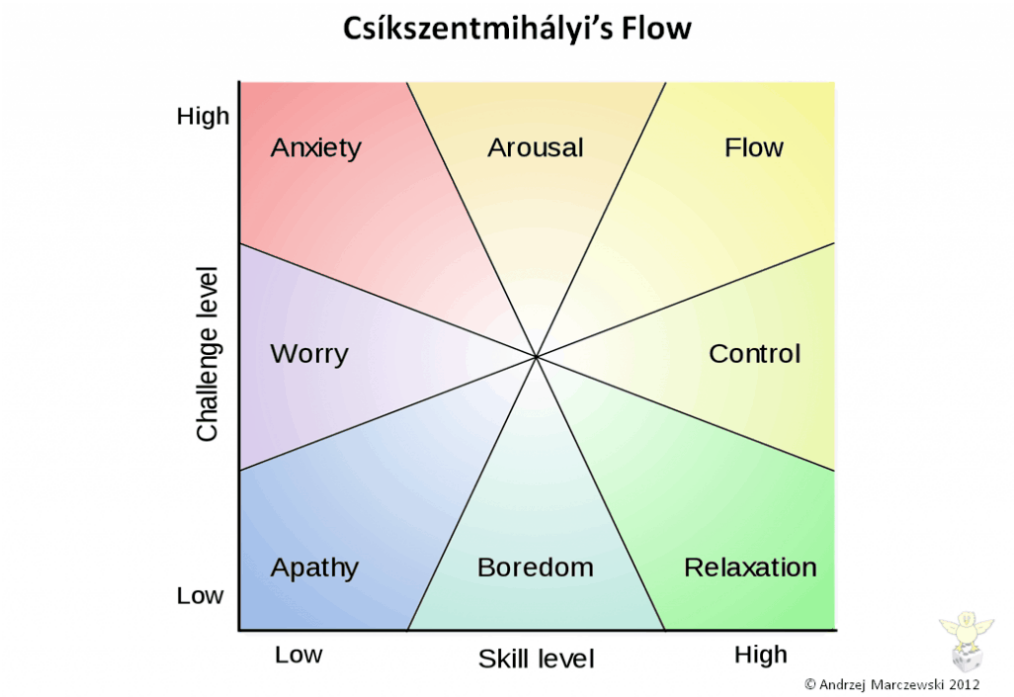

Figure 2.1. Flow graph (source: Gamified UK).

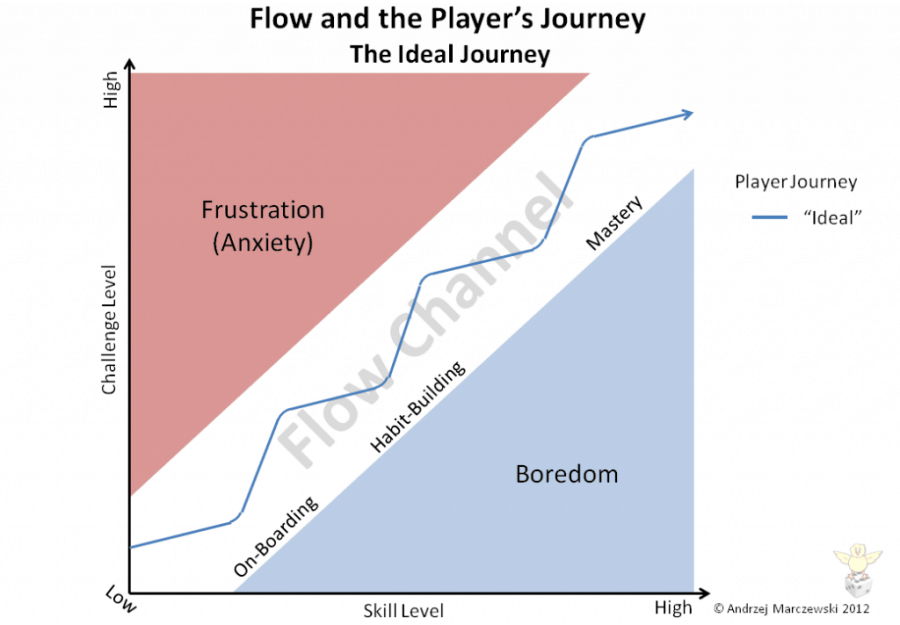

Figure 2.2. Player Journey (source: Gamified UK).

2.1.2 Self-Determination Theory

The Self-Determination Theory (SDT) explains some mechanics in relation with the human psychological needs: **competence**, **autonomy** and **social interaction**. These elements make possible intrinsic motivation. SDT theory underline the importance of the environment, feedback, time and reference (individual and social) to create motivation [23].

The SDT distinguished in intrinsic and extrinsic motivation:

- Intrinsic:

  Intrinsic motivation is defined as the doing of an activity for its inherent satisfaction rather than for some separable consequence. When intrinsically motivated, a person is moved to act for the fun or challenge entailed rather than because of external products, pressures, or rewards [24].

- Extrinsic:

  Extrinsic motivation is a construct that pertains whenever an activity is done in order to attain some separable outcome [24].

It is well known that intrinsic motivation, if it is possible use it, is more powerful than extrinsic motivation, because the user recognizes the task as useful or interesting for himself. Extrinsic motivation can cause addiction in case it is not well monitored. However, both are necessary, and a correct balance can be used in a gamified process.

2.1.3 Gamified Learning Theory

The Gamified Learning Theory was developed to underline the use of gamification in the educational field. The main idea is that gamification cannot replace the learning process but can improve it. There exist two factors process for which the game elements can influence learning: **mediating** (direct process) and **moderating** (indirect process) [25].

Following the figure 2.3 the mediating process is created thanks to the path:

```
D > C > B and A > C > B.
```

The moderating process is represented by the path:

```
A > B with the influence of D > C.
```

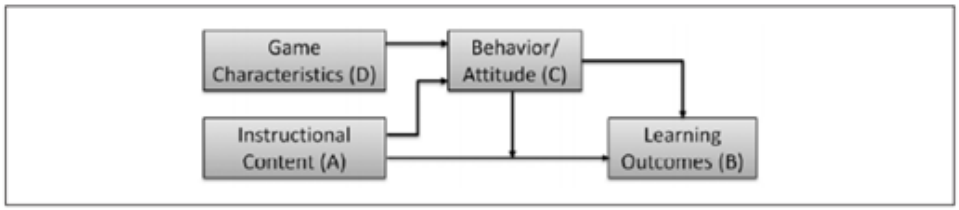

Figure 2.3. Gamified Learning Theory (source: "Developing a Theory of Gamified Learning: Linking Serious Games and Gamification of Learning").

The relation between the elements in figure 2.3 are the following:

1. Instructional Content (A) influences learning outcome (B) and behaviour (C). Instructional features change from context to context but if the instructional content does not help the learning process the gamification cannot resolve the issues.

2. The behaviour (C) influences the learning outcome (B), for example increasing the active students' participation can lead to more immersion and feeling of control. On the other hand, passive learning gives less benefit to learning outcomes.

3. The game characteristic (D) affects the change of behaviour (C). For example, increasing the difficulty level can encourage the creation of new strategies, ability and specific rules can increase motivation.

4. The game elements act on the behaviour that works on learning outcome efficacy, at the same time the use of game design elements increases immersion that works on the relationship between instructional content and the learning outcome.

   `(D > C) > (A > B)`

5. Relation between game elements (D) and learning outcome (B) is led by the behaviour (C). For example, the time spent studying can be incentivized by game mechanics and dynamics that create motivation, increase the time on task and therefore the learning outcome.

The paper [25] present also some examples of motivation and mediation:

- Moderation: The Professor adds narrative elements to the lessons already existing with the aim to motivate the students' attention.
- Mediation: The Professor adds narrative elements to the lessons to increase the time on task and the time dedicated to studying.

2.1.4 Fogg Behaviour Model

The Fogg Behaviour Model is a framework according to which the increase of motivation can be encouraged by triggers that avoid barriers of difficulty or simplicity [26]. The Fogg method has three elements: motivation, ability and prompt. These elements together can act on changing behaviour.

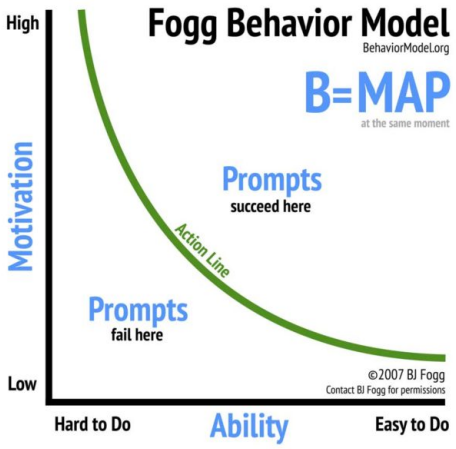

Figure 2.4. Flow graph (source: Fogg Behaviour Model).

The **behaviours** are divided in 3 types in relation to the execution time of a task [27]:

- Punctual: short term, action done immediately and only once during time (For example: invite someone the play at a game).
- Lapse: medium-term, action carried out for mouth/season (For example: follow a diet).
- Path: long term, modify a habit for the entire life (For example, give up smoking).

Some elements of **simplicity** that could help to change behaviour are:

- Time: schedule task during calendar.

- Brain cycles: mental effort to achieve a goal.
- Social deviation: social customs and social thought.
- Non-routine: break the routine.

Other important aspects underlined by Fogg are the **motivators** represented by pairs of emotions:

- Pleasure/Pain: immediate motivator, it represents the common human behaviour that tries to look for pleasure and avoid pain.
- Hope/Fear: based on users' ability in event prediction, hope is the anticipation of something positive/happy, fear is the opposite.
- Social Acceptance/Rejection: social acceptance is essential for individuals. Social media are based on this motivator.

The **triggers** are defined by Fogg as essential elements that interact with motivators:

- Spark: levels for demotivating users to highlight motivator factor as hope rather than fear.
- Facilitator: make a task easier, it is used when abilities are not yet enough.
- Signal: a reminder for strongly motivated users, to remain aligned with the already acquired behaviour.

2.1.5 Bloom Theory

The Bloom Theory is a hierarchical model used to organize types of learning in relationships with different difficulties levels [28]. It was theorized the first time in 1952 by Bloom, then it was revisited since nowadays.

It is organized into three domains: cognitive, affective and psychomotor. In gamification context, it should be useful its use to organize the lecture content. The cognitive domain should be used to select starting user's knowledge and desired final user's level. The cognitive level chosen should be used to design user experience using the psychomotor domain and user participation and emotion thanks to the affective domain.

1. Cognitive: this domain categorizes the types of thinking skill from easiest to hardest. Each element is linked with specific verbs that specified the action done by the users in the considered thinking level.
    - Knowledge: remember information (observe, listening, named, locating, listing).
    - Comprehension: make sense of information (summarising, demonstrating, discussing).
    - Application: use information in a different circumstance but similar to the presented ones (manipulating, designing, experimenting).
    - Analysis: explore relationships with other elements and find putters (recognize trends).
    - Synthesis: use the information to create something new (inventing, modifying, combining).
    - Evaluation: compare and examine critically thanks to the available information (solving, judging, rating).
2. Affective: this domain considers the emotion levels and individual value.
    - Receiving: base knowledge received by passive interaction.
    - Responding: active participation and response.

- Valuing: value linked to elements based on previous knowledge and personal value, for example be sensitive to other people.
- Organising: order tasks based on priority values scales.
- Characterising: create abstract knowledge based on previous information.

3. Psychomotor: it is based on physics movement and coordination.
   - Imitation: users learn by watching and copying.
   - Manipulation: users learn by memorization and by following precise instructions.
   - Precision: users become more expert and choose the actions to do in a more precise way.
   - Articulation: users do more than one action together in a precise way.
   - Naturalisation: the actions performed are natural for the users.

2.2 Gamification and Frameworks

In this section are summarized the main frameworks developed to organize and create gamification projects. The frameworks presented are generic, and not created for a specific scope of application. For this reason, they are applicable in different contexts but at the same time general and not specific. Most of them keep into consideration distinct types of motivators, game dynamics and mechanics, user types, player journey. Others give hits, instruments and suggestions regarding how to implement the gamification experience and how to organize the development phase.

2.2.1 Octalysis

Octalysis, created by Yu-kai Chou, is one of the best-known frameworks in the gamification context. It defines eight core drives that represent the main sources of motivation [29].

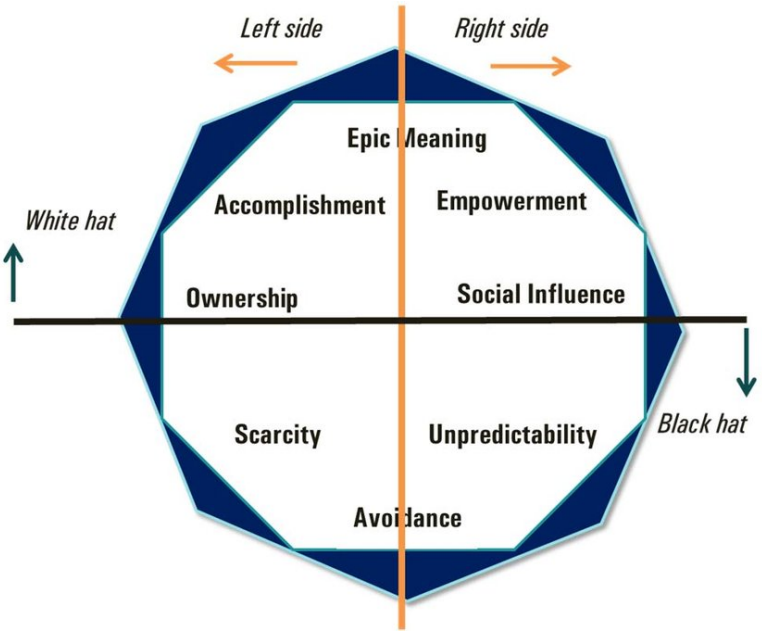

Figure 2.5. Flow graph (source: "Gamification in Education: A Methodology to Identify Student's Profile").

The core drives are:

- Epic Meaning: feeling of belonging to a larger project, the user recognizes his help as indispensable for overall success.
- Accomplishment: observation of progress and skills acquired.
- Ownership: possession and look for resources or earnings new things.
- Scarcity: the user is motivated to obtain something hard or impossible to achieve.
- Avoidance: actions that prevent some negative features or elements as the loss of resources.
- Unpredictability: the user is motivated thanks to the curiosity to discover what will happen in the future.
- Social Influence: social interaction and relatedness.
- Empowerment: the feeling of continuous improvement, the user engages in the creative process.

The schema should be divided in two ways [30]:

- Vertically. The section obtained on the right is named "Right Brain Core Drives", it represents intrinsic motivation, creativity and self-expression. On the other hand, the section on the left is "Left Brain Core Drives" that represents the extrinsic motivators more related to logic and calculations.
- Horizontally. The "White Hat" core drives are the top elements that represent a high sense of meaning, positive emotion and mastery skills. At the bottom of the framework, there are the "Black Hat" core drivers that are characterized by the feeling of losing something.

The framework is organized in three steps [29]:

1. At the beginning is necessary to analyse the system with the eight-core drives. For this purpose, is available a tool that helps to visualize the analysis. It is possible to assign to each driver a score between 1 to 10 based on personal ideas.
2. The second step is concentrated on the analysis of the different phases of user experience (discovery, onboarding, scaffolding and endgame) always related to the core drives.
3. The last phase is dedicated to the study of user topology (Achievers, Explorers, Socializers, Killers) during the whole path described in the second phase

This framework can be useful to analyse an existing system and understand the motivator aspect needed. It is possible to see an example of its use in the figure 2.6, on a well-known system like Facebook.

2.2.2 MDA

The MDA framework is a formal approach that divides the game concepts into key elements: rules, system and fun. MDA establishes the design related items: Mechanics, Dynamics and Aesthetics. **Mechanics** are defined as game base elements. **Dynamics** are the mechanics behaviours run time activated by input or output elements. The **aesthetics** are the player emotional responses caused by dynamics [31]. It is important to notice the different perspectives between developers and users. The designer directly intervenes on the mechanics that work on dynamics and create aesthetics, instead the user perceives as first the aesthetics and then the reverse path up to the mechanics' 2.7.

The emotional component is essential in a gamified system, [31] defines the principal aesthetics taxonomies:

- Sensation

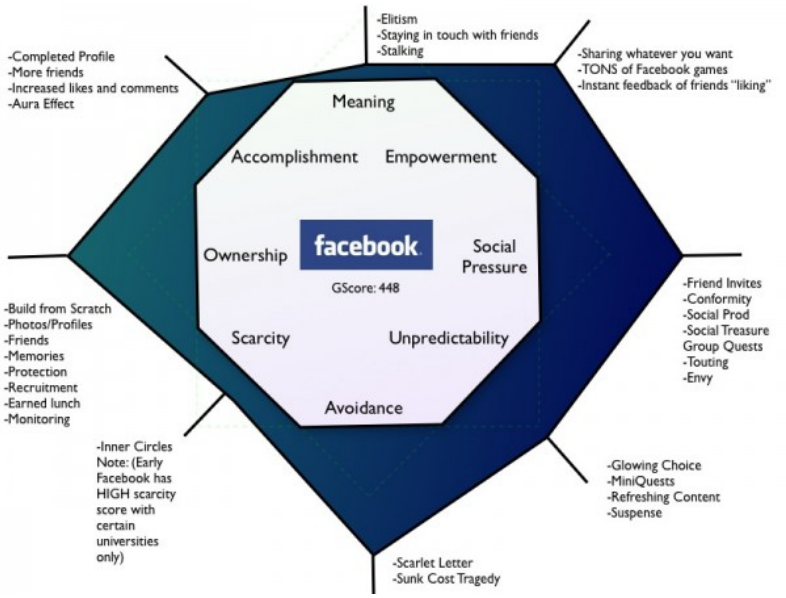

Figure 2.6. Octalysis analysis on Facebook system (source: The Octalysis Framework for Gamification & Behavioural Design).

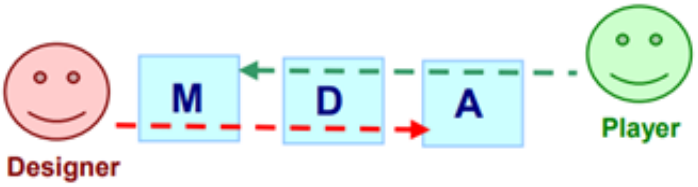

Figure 2.7. MDA graph (source: "MDA: A Formal Approach to Game Design and Game Research").

- Fantasy
- Narrative
- Challenge
- Discovery
- Expression
- Submission

Each game can have more than one taxonomy with different intensity levels.

The use of MDA framework should be necessary to define the desired aesthetics and establish the correct mechanics and dynamics for the taxonomies chosen. This method helps the developer to articulate the goals and design the system structure without losing the user prospective [32].

2.2.3 6Ds

6Ds framework is a design process that consists of six steps, each of which begins with the letter D [33].

1. Define Business Objectives: define which results are expected for the system and principal aims

- Concrete and an ordered list of goals.
- Eliminate irrelevant elements.
- Justify the reasons for the elements chosen.

2. Delineate target behaviour: what users have to do.
   - List of tasks for the users.
   - Metrics definition to evaluate the system.
   - Evaluation method definition.
3. Describe your players: both master data and characters. In order to describe the users can be used the player analysis, which distinguishes achievers, explorers, socializers and killers. This phase is useful to define the correct elements suitable for users.
4. Devise activity loop, this step is important to increase the player skills inside the system.
   - Engagement loops: how to motivate users to repeat actions.
   - Progression loops: define the player journey.
5. Do not forget the fun: the fun creates engagement and intrinsic motivation.
6. Deploy appropriate tools: choose the correct platform or system to deploy.

This approach is used in many applications and helps to organize the work in different fields and areas of interest.

2.2.4 User Types and User Journey

Users can be categorized according to specific attitudes. One popular study divides the users into six groups: Disruptor, Free Spirit, Socialiser, Philanthropist, Achiever and Player. For this reason, the framework is named **User Type Hexad** [34] [35].

Figure 2.8. User Type Hexad (source: Gamified UK).

- Philanthropists: motivated by purpose and altruism. Elements: collections, share knowledge, rewards.

- Socializers: motivated by social relations, interaction. Elements: teams, social network, competition, comparison.
- Free Spirits/ Explorer: motivated by autonomy, free speech, creativity and customization.
- Achievers: motivated by competence and challenges. Elements: challenges, badges, levels, progression and boss battles.
- Players: extrinsic motivation. Elements: rewards, leader-boards, badges, virtual economy, lottery.
- Disruptors/ Killer: motivated by recognition of changes. Elements: new platforms, vote, anonymous, anarchic game.

Another important aspect to keep in consideration is the evolution of the user during the usage and the discovery of the system. There exists a framework named **EEEE** that divide the user phases inside the system:

- Enrol: first entry into the system, other studies call this phase "onboarding". The user decides to use the system.
- Enthuse: phase of enthusiasm to try and discover the system.
- Engage: users start interacting with the system in the way desired, more conscious and focus on aims.
- Endear: at the end of the journeys the users keep using the system only if intrinsically motivated.

During these phases, the learning curve is growing till the engage phase, then it risks going down if the motivation decrease. For this reason, a careful analysis of user, player journey and the relation between them is important for the success of the platform [36].

2.2.5 Gamification Model Canvas

The Gamification Model Canvas is based on Business model canvas, MDA framework and the last release, also include the Fogg Theory. It exploits theories based on motivation and user-type models. The goal is to combine in a single model the choice of mechanics and dynamics thanks to the MDA based on the types of users both considering their experience inside the system, both considering their typical characteristics and consequently the most suitable motivators. The inclusion of the Fogg theory includes also simplicity or difficulty of each element in order to analyse the correct usable and useful trigger to stimulate different types of users. It was created to develop gamified system and to help the designer to choose the correct element [37]. As shown in the figure 2.9 the model is divided into ten sections, the developers can add their comments and choices for the system directly inside the figure during the design phase.

The first version was made up of nine sections:

1. Revenues: economic or social return obtained thanks to the system and the gamification introduction.
2. Players: choose a specific target and describe the users using the user type model.
3. Behaviours: specific behaviour or action desired for users, underline which behaviour you want to change.
4. Aesthetics: emotions aroused in users when they interact with the system.
5. Dynamics: mechanics run-time behaviour during the time.
6. Components: describe the game elements and features to create feedback and mechanics.

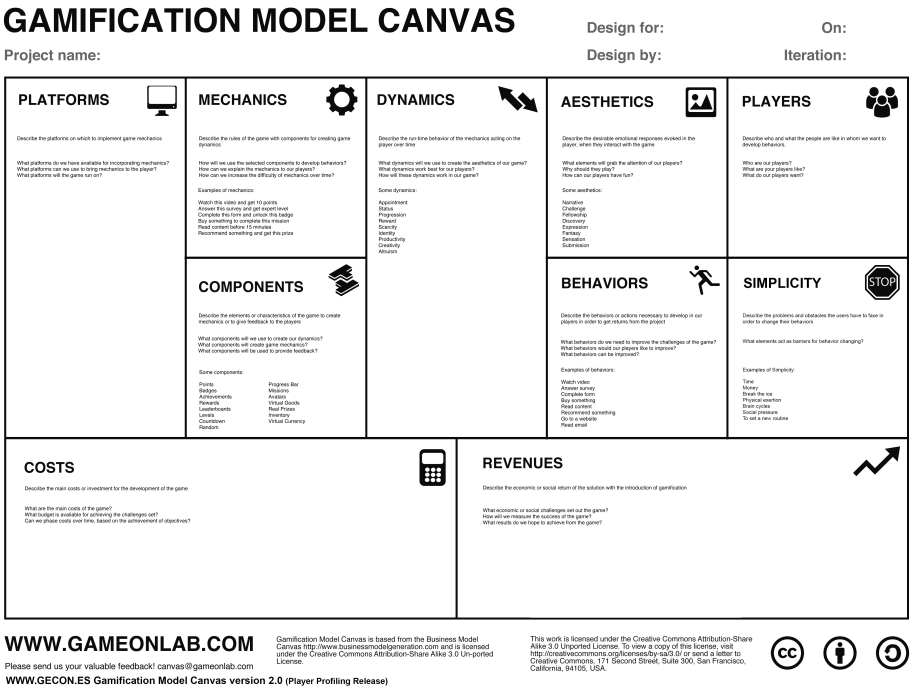

Figure 2.9. Gamification Model Canvas (source: Gecon).

7. Mechanics: game rules created thanks the behaviours to crate dynamics.
8. Platforms: platforms, software and hardware used to implement the system.
9. Costs: investments for the project.

This solution keeps into consideration two main aspects:

- The game: in the right section there is the player that perceived the game through aesthetics and dynamics, in the left section there is the designer/developer that builds the game starting from mechanics inside the platform to create dynamics. This focus is based on the MDA model.
- Business: the system is also focused on efficacy and the project value. The right section represents the value for the gamer, the left part represents decisions for efficacy and costs. This aspect is considered following the canvas business model.

The second version of the model was created by adding the **simplicity** element, following the Fogg theory. With this element, the model analyses also the difficulty or simplicity of each element and the possible triggers. This model also includes the Persona method focus on precise identification of the target, creating the Fogg Persona System (FPS) [38]. FPS incorporates simplicity, motivation, self-determination, and the evolution of user capacity. In order to create the model FPS is used an involvement index named **Gamification Model Canvas Level** with three levels: **high**, **medium** and **low**. Compared to the Player journey is possible to relate the low level with the newbie/onboarding users, with the medium level the master/engage users and with the high level endear users. The levels are used to represent each aspect of the game: players and profiles, simplicity, motivations, behaviours and dynamics.

This framework, with its evolutions, is the most complete for the general gamification process. It is based on the gamification main theories and also considers the user journey. The only missing aspect is the evaluation metrics.

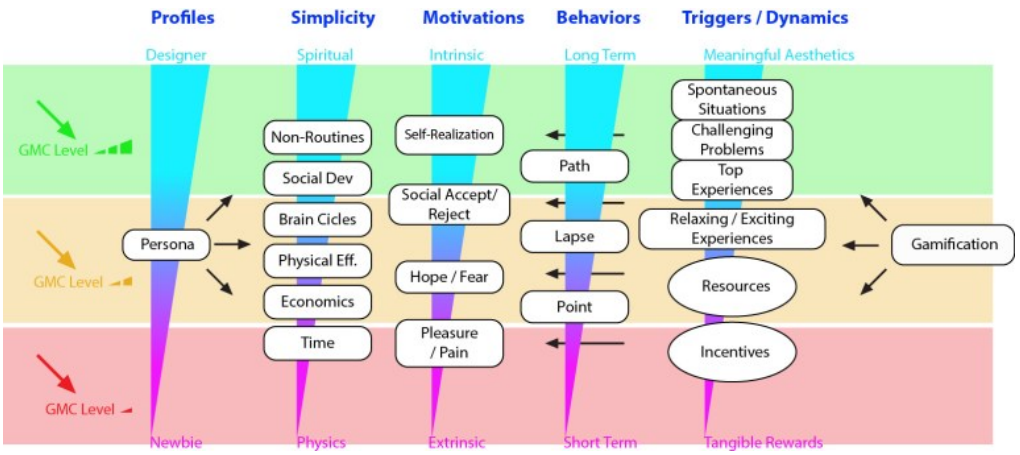

Figure 2.10. Fogg Persona System (source: Gecon).

2.2.6 Sustainable Gamification Impact (SGI)

The SGI framework has the aim to make the gamified system sustainable during the time, in the extended period [39]. It is based on Flow Theory and Self-Determination Theory. The model analyses three base concept: the **flow** as competence and skills that induct the intrinsic motivation, the **motivation** as autonomy, fun and control, at last **engagement** as user involvement.

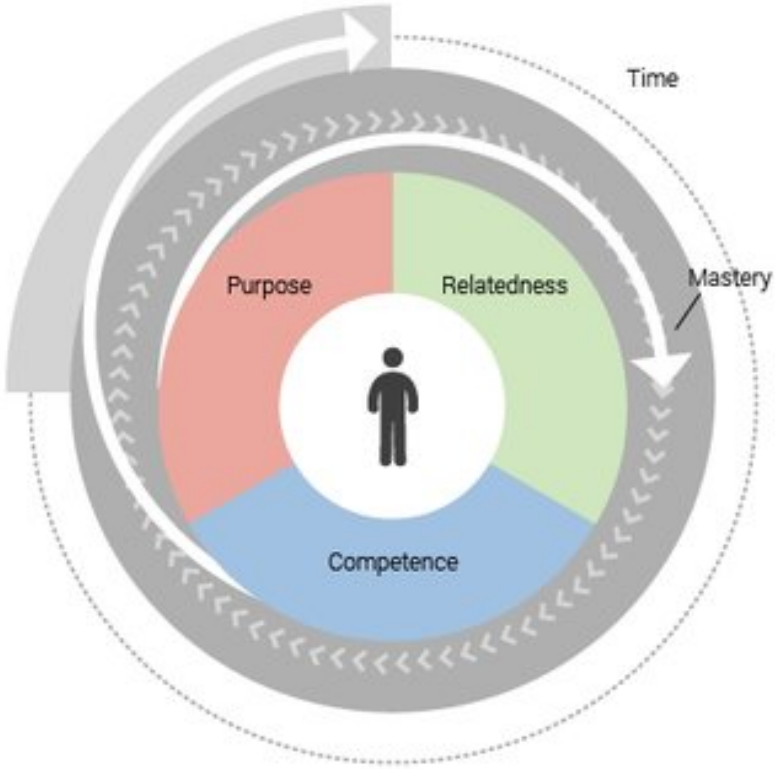

Figure 2.11. SGI framework (source: "SGI: A Framework for Increasing the Sustainability of Gamification Impact").

The figure 2.11 represents the framework that uses a spiral loop: at the beginning is necessary to study the needs, relations, skills of the users. The spiral concept is used to underline the idea

that a user must never return to a previous point already acquired. The aim is to bring the user to an expert level in the field analysed.

- Relatedness: relation with other users, the inclusion of socializer elements.
- Purpose: self-learning with clear aims and meaningful feedback.
- Competence: feeling freedom and ability to make decisions.
- Mastery: desire to improve themself and their skills. The user needs to see their progression over time.

The framework should be used both in **developing stage**, to check if the requirements are fulfilled, and during the **evaluation phase**, if the system already exists SGI can be used to analyse and modify the system and monitor the direct user experience.

2.2.7 Moar

The Moar schema is used to explain the engagement loop [40]. It consists of four elements: motivation and interest, opportunity, action and response.

- Motivation: it is necessary that the user has an initial interest or curiosity related to the topics or product proposed.
- Opportunity: create the correct condition to give to the users the possibility to do the action desired. This aspect is also related to the user's abilities and skills in a specific moment.
- Action: actions that users must carry out to complete the tasks. Users can see the actions like missions or challenges.
- Response: to satisfy humans' need to receive a reaction because of an action, is important to create immediate responses after action as feedback. The response closes the engagement loop but also should create emotion in the user in order to turn this emotion into new motivation and, in this way, start a new loop. On the other hand, missing feedback may disengage users in starting a new loop.

2.2.8 REF Schema and SAPS Theory

An important topic in gamification is the rewards system, how to encourage users and motivate them with external stimulation. For this purpose, it was created the REF schema, that is means Reward Engagement Framework. It is based on two elements: which reward is used and the timing of award [40]. Gabe Zichermann created the SAPS theory. SAPS is an acronym that sums up the main way to reward users: Status, Access, Power and Stuff [41].

- Status: create a ranking between users based on experience or skills. Status should be recognized by other players often using badges, levels or leader-boards.
- Access: gives access to content otherwise unavailable. In this way, the user can interact in an exclusive manner with the system. This is often created with a VIP account that gives more choice possibilities.
- Power: role and career growth inside the system, user receive the ability to carry out preferences action. For example, he can become a moderator or obtain privileges to delete inappropriate comments inside a forum.
- Staff: the user receives objects or services. They are considered as real awards, however, is the reward that creates less loyalty between the system and users. Moreover, it is not always easy to create a correct staff system because also requires an economic effort compared to other elements. On the other hand, users have to recognize a correct balance between the staff obtained and the effort in the actions done.

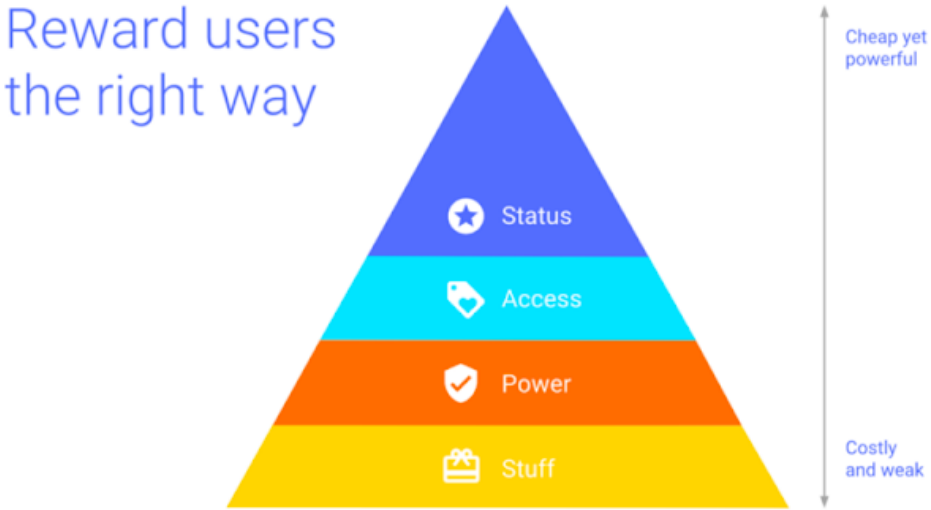

Figure 2.12. SAPS framework (Major Project).

The SAPS system is often represented by a pyramid 2.12. It is important analyse the type of rewarding in the specific order to create more engagement during the experience path in the system and monitor the cost. Paradoxically, the highest steps of the pyramid are cheaper and give more engagement compared to the last steps.

There exists another type of rewarding that is related to the **emotional rewards**. If the user feels belonging to a group and his actions help the community some forms of gratitude are enough to make the user feel satisfied [42].

Other reward types come from the video games world and should be applied in the gamified context [40].

- Currency Rewards: use virtual coins inside the virtual platform with the purpose to purchase new products or skills.
- Rank Rewards: change of status between one level and the next one.
- Narrative Rewards: discovery of new elements of a story during the game path, for example once the user gets badges, he receives a narration chapter.

Relate to reward is important analyse not only the type but also keep in consideration how rewards are delivered [42].

- Constant Rewards: user knows that will receive some form of rewards after some specific actions, or a constant period.
- Random Rewards: user knows that he will receive an award, but the content is unknown, for example the birthday gift.
- Lottery: only a portion of the players will be rewarded, for that reason the prime size is greater.
- Sudden and Unexpected: some unknown trigger activated the rewards system, for example Easter eggs.

2.2.9 Development Cards

There are some cards created to help developers to choose the correct game elements in different situations. Fabio Viola create the "Engagement Deck", which is a deck of cards with one hundred and one techniques with the aim to improve the user experience in gamified process [43]. On each card there is the technique and some useful information that gives hits to the developers about when choosing the cards:

- **Player type**: the symbols A-E-K-S represents the four types of players (Achievers, Explorers, Killers, Socializers). On each card is indicated for which type of user the technique is best suited.
- **Player phase**: I-II-III-IV, these phases represent the user journey. This element helps the developer to choose the technique in relation to the user experience inside the gamified product.
- **Benefits**: this section summarizes the most benefits that the technique has (For example: change of behaviours, entertainment)
- **Dynamics**: the section reports the motivational driver used by the technique.

Figure 2.13. Engagement Deck (Gamifications).

Another similar, but a more recent product, is the "Playable Cards" created by Fabio Viola and ProjectFun [44]. The playable project defines 133 cards to help the development phase. They are focused on:

- Player type (six different players type)
- Player phase (four phases in the player journey)
- Dynamics
- Strategic goals

2.2.10 LM-GM

The Learning and Game mechanics framework for serious games [45], has the aim to create a relationship between game mechanics, game patterns and pedagogical content, linking fun and pedagogy. The model is general and not created for a specific environment with the aim of defining the right proportion of fun and knowledge.

The model proposed a table 2.14 with training mechanics and game mechanics. The model is descriptive, in the sense that it leaves the developer free to join mechanics of play and learning by his opinion.

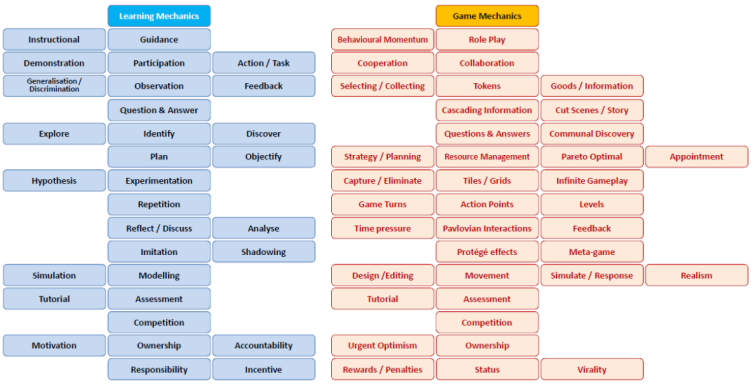

Figure 2.14. LM and GM used to organize the serious game experience (source: "Mapping learning and game mechanics for serious games analysis").

The model proposed two elements to organize the experience:

- Static table, created to organize and link mechanics game and content with implementation information. The table should have four columns: Game mechanic, learning mechanics, implementation, usage.
- Map, used to represent dynamically relation between LM and GM during the game phases

The model directly includes the Bloom Theory in order to organize and categorize knowledge levels as it is possible to see in figure 2.15.

2.3 Theoretical Results from Previous Studies

Thanks to previous studies, it is possible to summarize some interesting elements to keep in consideration in a gamified experience. First of all, it is not easy to choose the correct game element to include in the project, but results report which elements are considered more suitable than others in relation to the context of applications. In this section, it is also analysed the freedom element, considered as fundamental within a project with gamification. In conclusion, it is possible to find analyses of a special type of gamification in urban contexts.

2.3.1 Game Design Elements

One of the most important parts of gamification is the selection of game elements based on the desired behaviour and outcome. The correct elements can motivate or discourage an action, this choice is also related to the type of users: target, skills level, previous knowledge, characters. In the figure 2.16 there are represented the main gamification elements divided by the user type [46].

The comparison of previous resources defines the most important elements [47]:

GAME MECHANICS	THINKING SKILLS	LEARNING MECHANICS
○ Design/Editing ○ Infinite Game play ○ Ownership ○ Protégé Effect ○ Status ○ Strategy/Planning ○ Tiles/Grids	CREATING	○ Accountability ○ Ownership ○ Planning ○ Responsibility
○ Action Points ○ Assessment ○ Collaboration ○ Communal Discovery ○ Resource Management ○ Game Turns ○ Pareto Optimal ○ Rewards/Penalties ○ Urgent Optimism	EVALUATING	○ Assessment ○ Collaboration ○ Hypothesis ○ Incentive ○ Motivation ○ Reflect/Discuss
○ Feedback ○ Meta-game ○ Realism	ANALYSING	○ Analyse ○ Experimentation ○ Feedback ○ Identify ○ Observation ○ Shadowing
○ Capture/Elimination ○ Competition ○ Cooperation ○ Movement ○ Progression ○ Selecting/Collecting ○ Simulate/Response ○ Time Pressure	APPLYING	○ Action/Task ○ Competition ○ Cooperation ○ Demonstration ○ Imitation ○ Simulation
○ Appointment ○ Cascading Information ○ Questions And Answers ○ Role-play ○ Tutorial	UNDERSTANDING	○ Objectify ○ Participation ○ Question And Answers ○ Tutorial
○ Cut scenes/Story ○ Tokens ○ Virality ○ Behavioural Momentum ○ Pavlovian Interactions ○ Goods/Information	RETENTION	○ Discover ○ Explore ○ Generalisation ○ Guidance ○ Instruction ○ Repetition

Figure 2.15. Classification based on Bloom's thinking skills (source: Mapping Learning and Game Mechanics for Serious Games Analysis).

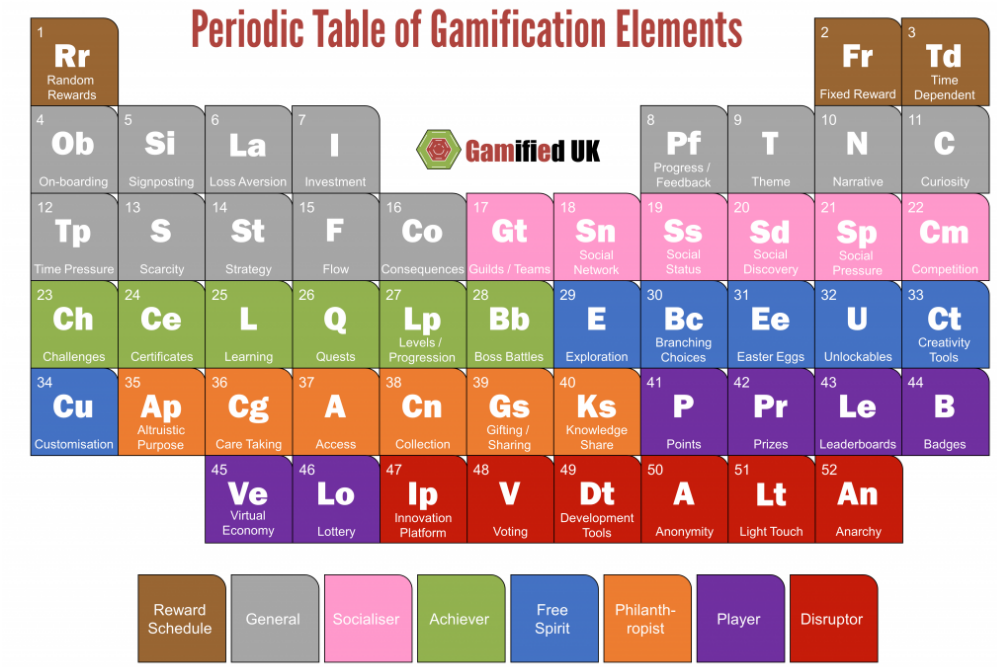

Figure 2.16. The Periodic Table of Gamification Elements (Gamified UK).

Social Interaction and in particular the competitive-collaborative aspects. Competition is difficult to evaluate in an environment with different users' level skills, anyway, is important to keep in consideration. The collaborative aspect is defined as the ability to work in a team with a common goal and it is relevant both for relations and skills. Competition is divided into destructive and contractive, the increase of social pressure to achieve an improvement of kills level should be raised by both competition types.

Period of time, the study report significant results for the gamification process in a long

period: more than one month, half a year or more. Instead, a short gamification program, as one day, one week or less than a month, does not report important outcomes but in some cases points out a decrease in results compared with the standard process.

Research context, the school setting is preferred but there is a possible bias related to ease of analysis and data collection in a school environment rather than in a working setting.

Game Fiction does not report important outcomes for the cognitive and motivational results but for the behavioural aspect should be taken into consideration.

In the education context the game design elements recognized by experts as most relevant are [48]:

Objectives, that affects both motivation and engagement and is defined as the guide of the player actions like maps, tutorials or paths.

Levels, represent the user path inside the game and gradual growth, this aspect engages the users.

Progression, to increase the engagement the users need to visualize the progress thanks to a progression bar or a map.

Narrative, is defined as the order of events during the game, chosen action and user strategy to complete levels. This aspect represents also the freedom in choosing the path during the experience, to be free to choose actions to increase the user motivation.

Storytelling, is how the story is narrated using voice, text, video or direct experience. This aspect is important for user engagement.

It is well known that motivation favours concentration, attention and memorization. A study based on already existing gamified system analyses and links motivators with the game mechanics [49]. It distinguishes motivators in ten categories: **autonomy** preference to be independence in choice, **power** desire to direct, be admired and win, **achievement** overcome the challenges, **exploration** find new way to do things, **contribution** desire to help other users, **affiliation** feel part of a group, **cooperation** equity in the relation and help each other to obtain the same goal, **hedonism** save user effort and avoid to sacrifice personal well-being for an external aim, **security** system balance and avoid uncertain changes and **conservation** protection of own resources or points.

The cooperation is related to the **sharing knowledge**, **exchangeable points** and **group challenges**. The power elements are related with mechanics linked with **boss battle**, **competition** and in **voting** and giving system feedback. It can also be represented by **badges** that works on the need of success and its external recognition. Another game element related to the power is the **leader-board**, which should be seen as power expression. Achievement motivator is triggered by **challenges**, **rewards**, **unlock sections** and visualize **progression** during the path. Creating a daily appointment, or more in general a specific and fixed ritual, create affiliation with the platform. The ability to customize the own account or chose the **avatar** may be experienced as a freedom and autonomy element [49] [50].

Another important mechanic is the **progress-bar**, this is based on two cognitive bias named Zeigarnik Effect and Endowed Progress Effect [51] [52] [53]. Thanks to the Zeigarnik effect, humans tend to easier remember incomplete actions or tasks. This is used, for example, in TV series during which each episode ends with an open question. On the other hand, the Endowed Progress Effect explains that people are more incentive to do an action if it is already started and if the proximity of the prize seems easily reachable. Complete action already started is easier than starting a new task from zero.

These biases can be exploited in two ways:

- On-barding phase: using a to-do list with the first action already checked as completed.
- Progress-bar: to incentive users to complete levels or actions, the users feel satisfied when completing a task.

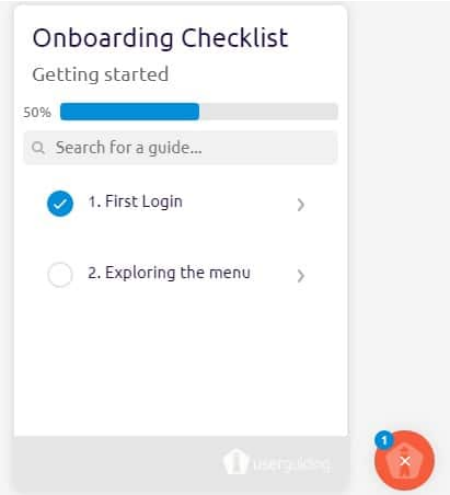

Figure 2.17. On boarding to do list and progress bar (source User Guiding).

2.3.2 The Freedom Element

The gamification process automatically includes the user freedom aspect. Scot Osterweil theorized the so called "The Four Freedoms of Play" [54]. Osterweil explains how learning and motivation work inside the game and he theorizes four freedom that it is necessary to respect to obtain the best result in the gamification process and to create an environment as close as possible to the game atmosphere. The goal is that thanks to the freedoms, users recognize the game environment.

- Freedom to fail: the users can fail without punishment or consequence. It must create contrast with the real world. The "carrots and sticks" method does not work in a gamified system.

  > There is no better teacher than failure, and there is no better environment for failure than that of a game.

- Freedom of experiment: in the real world people are not encouraged to experiment with new strategies if the habits work. Instead, in the game environment is possible to try and find innovative approaches.

  > There is no cost to try.

- Freedom of identity: users are free to choose which role impersonate, to create a new self-identity in a novel world. Again, this aspect moves away from what happens in the real world in which society requires fixed and predefined roles based on environment and social contractions.

- Freedom of effort: each user is free to choose how much effort to dedicate to the game, players can take breaks anytime they want without any external impositions. User is also free to choose whether to play or not to participate.

2.3.3 The Fun Theory

Concerning the application of gamification in a different way than video games or similar, there is the fun theory. It does not use any devices or virtual games but is based simply on making fun. Following the idea that making fun of people can change their habits, Volkswagen funded an advertising campaign in Sweden that applies The Fun Theory to everyday life [55]. This application is also defined as urban gamification. To encourage people to make healthier habits for themselves and others, they simply change some urban elements, usually not considered or considerate boring, only triggering curiosity and fun in users.

Here there are some examples of this application:

- Piano Stairs: inside an underground station they change the normal stairs with a playing piano: each step corresponds to a note. After this experience more than 66% of users prefer the use of stairs instead of the escalator 2.18.
- The World's Deepest Bin: each time that users throw something in the trash the bin makes a sound that mimics a deep pit.
- The Speed Camera Lottery: thanks to an ideas competition it was created a speed road detector that fine who exceeds in speed and gives a lottery ticket to those who respect the limit. The lottery is financed by fines collected for speeding. The average speed before the experiment was 32 km/h and during the experiment 25 km/h, with a reduction of 22% of speed.

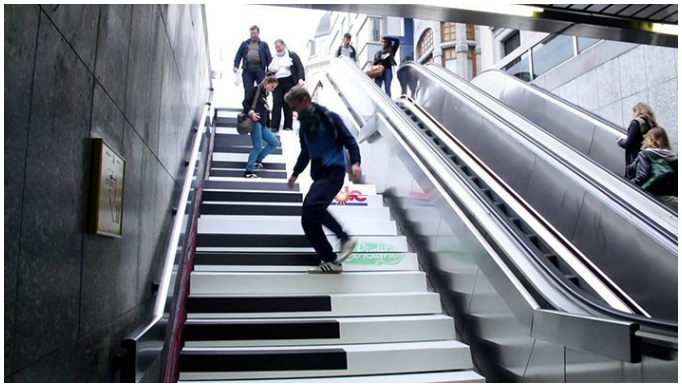

Figure 2.18. The piano stairs of the fun theory(source Design Playground).

Another similar project related to urban gamification is PlayableCity [56]. This project developed and installed some gamified experiences inside cities to make the urban environment more attractive, interactive and make citizens happier. This idea has the purpose of thinking differently about the own city, both in terms of tourism and for everyday life. It is possible to find PlayableCity installations in all over the world.

Chapter 3

Application in Cyber Security Field

3.1 Why Use Gamification in Cyber Security

As mentioned in the introduction section, an increase in training in the cyber security context is necessary. It is important, both for personal reasons and for company business, that users can defend themselves from the most common attacks and vulnerabilities.

Cyber security education, when is applied, often presents problems because it is concentrated only on theoretical concepts. It is important to learn cyber security theoretical elements but is essential that employees comprehend how to act practically in front of dangers. Even more important is to train users to recognize dangerous situations. It is relevant that the cyber security training and awareness program concentrate the effort on changing behaviours [57]. All these elements are supported by research that arise the fact:

> People know the answer to awareness questions, but they do not act accordingly to their real life.

In order to change behaviour is important to avoid and prevent mental shortcuts, the use of defaults element can help because our brain tends to follow preselected options. The use of emotional association can induce user actions more strongly. Exploit the human ego for security benefit can be a strategy: people often act in the way to fill their actions or their feelings as best both compared to the other users and themselves paste actions. The social environment and cultural elements can interact with the human choice, messages or advertising that respect the cultural model of the receiver may work in this way.

An important technique is persuasion that works in two main ways: to influence the human thought about an event in a rational way or to make a process automatic without changing the thought. Classical implementation of persuasion includes the principal emotions, anyway it was proved that the induce a sense of fear is usually counterproductive [57].

A successful approach in the cyber security environment includes a correct target understanding, global vision of the problem, use of correct material performance measurements. For these reasons, comparing the gamification features, it seems clear that gamification is a possible path to success.

Another essential element, theoretically manageable with the use of gamification, is the concept of usable security [58]. This model includes each type of user, prefers the use of an appropriate vocabulary related to the target and avoids technical words for non-technical users. The system must have feedback and helping system definition. Users must be informed about the current security system and the security features need to be visible and available to reduce the user mental effort. Every system should be evaluated both by a security expert team and by users.

The user evaluation may be performed by analysing the use of tools during laboratory, survey or by observation.

According to [59] the main methods used to create a security awareness inside a company are web-based or virtual classrooms session, periodic newsletters, messages and alerts, cybersecurity week or events, warning banners or messages. These techniques raise some related problems:

- Long learning sessions concentrated in few moments. This element underlines different problems: the users cannot memorize actively many topics at once. On the other hand, the learning process is not continuous and updated this is a problem both for the content and for the learning aspects. The content of the material needs a periodic update, considering new vector attacks, types of vulnerability and methods of defence. For the learning process repeat the same content several times, in different way and context help the memorization and the active actions performed.
- Use a not realistic environment, the user must be able to find and know how to act personally recognizing the possible actions in his daily environment.
- Often the instructor is a technical security expert, with great knowledge but a bed communication ability.

The use of gamification in cybersecurity is supported by [60]. The use of gamification can help to create more effective knowledge and reinforcement of skills that if not applied directly could be easily forgotten. Also considering the knowledge retention rate about the learning method used is clear that gamification is a good strategy: immediate application in a real situation has the 90% of retention rates, practice by doing the 75%, compared to the 20% of audio/video, 10% reading and only 5% of hearing a lecture.

The use of gamification in cybersecurity fields has different purposes. For example, it is possible to reduce the time of education: as reported by [61] it is possible to reduce from seven years of standard education to two or three years based on CTF competition, with the same technical knowledge.

The integration of gamification in cybersecurity is also training for the work environment, during with it is normal to work in a team with different hard and soft skills. Obviously, it is possible to distinguish between two types of education and game-based experience: security awareness and expert education. It is clear that the two types of application differ for target, interest and purpose but they have in common the application needed, and gamification can give these skills.

The use of gamification should also approach new target as technical experts like young people and women, in a sector that every day need a new workforce.

The reasons why it is necessary to include gamification in the cybersecurity education program are [62]:

- Immersive content
- Increase course completion and participation
- Increase engagement
- Help the change of behaviours

These elements are supported by [63] gamification survey. What has emerged is that workers feel more productive for 89% and happier for 88% at work. 83% of workers trained with gamification feel motivated, compared to 61% with standard training feel bored. An interesting data is that 43% of employees trained with gamification elements did not notice that. Thank to this statistic, it is also possible to notice that employees' perception of gamification improves over years.

3.2 State of the Art

In this section are presented gamification projects only related to cybersecurity topics. The purpose is to see which kind of applications exist and what results were found. The existing projects are mainly designed for education, work and private environment. The section organizes the content distinguished in these three areas of interest because the environments change both the cybersecurity purposes, learning content selected and the gamification design, game elements selected and motivators.

One limitation of this analysis in the thesis context is the use of serious game elements in contrast with the use of gamification. The creation of a real game or simulation is categorized as a serious game. Gamification is defined as the use of game elements to create immersion without the necessity to create a real and complete game [64]. The gamification includes **game thinking** and **game elements**, instead serious game world also includes **game play**. The section focuses mainly on examples of gamification, but it is also possible to find some elements related to serious games. Their analysis intends to present as fully as possible the existing panorama related to the cybersecurity world useful also for a later generalization.

3.2.1 Company Environment

Some companies try to increase their security training and awareness programs by experimenting the gamification. The first aim is to change motivation, knowledge and behaviour to increase the company security. One method used is to create a gamified system with the integration of different game design elements to increase the motivation of more users as possible. According to [65] the use of gamification increases by 50% more phishing recognition and by 82% more of reporting. In general, reduce the risk related to password, phishing and malware by 10%. Another aspect theorized by [66] is the user participation and user perception of gamification effectiveness. According to this study, more than 75% of users suggest gamification education. This aspect should be also related to the new worker generation, because typically they are already familiar with the game and computer system world since their childhood [63].

Here are reported some examples of projects that try to use gamification to increase or change cybersecurity culture:

1. The study [19] creates a gamified platform to educate employees about phishing attacks. The standard method used was the emails system. To analyse the effect of the gamification, the employees are divided into three groups: standard education with emails, education with gamification and a control group that does not receive any type of education. The content uses in standard and gamified education is equal, employees receive the same kind of information. After six months all the users were tested with a phishing email especially created to control the user behaviour.

   In the control group, the 44% were phished, in the email group about 40% replay of to the phishing email and the user in the gamified group replay the attack only for 27%.

   In conclusion, this study underlines two main things:

   - Standard and passive education are quite similar to non-training at all.
   - The relation between challenge and immersion in gamified environment follow and U-shape trend. On the other hand, in a non-gamified system, the use of challenge is lived as frustrating, instead of in a gamified system is motivating.

2. The final user's collaboration and involvement since the first steps are needed to choose the correct elements to be included in the gamified system and reduce the number of cognitive biases [67]. This application involves users with three steps: a first **interview** with employees to collect data about the standard education and two workshops. The **first workshop** identifies the business desired outcome for the company and the motivators user's factors. During the **second workshop** an interactive prototype of the system was presented, users can interact with it and give feedback to improve it. A key factor used in this experiment

is the use of concise information, the micro-learning teaching technique is used as the main educational approach [68].

According to the users:

- It is preferable to use analogies to make the material more comprehensible also to not experts. It is suggested to make users able to visualize and understand dangers.
- The use of real stories with the description of actually occurred incidents, problems and errors.
- Avoid user procrastination at the last available minute but induce constant use.
- Users can report and ask for help at any moment.

3. Nearly all applications analysed use web applications specially created but they do not extend or include the everyday system. As reported in [65], could be used three different platforms for the application: **learning platform** to understand the actual knowledge, **performance-based platform** that integrate the system used daily in this way is possible to monitor the current behaviours and **custom system** created ad hoc. It is clear that each company and environment need a personified system according to needs but gamified the everyday system interaction could exploit the potentiality more completely.

   Following this idea, Autodesk and Elevate Security [69] created for employees a personalized dashboard: Security Snapshot. **Security snapshot** monitors and improves employees' knowledge on security. They focus on four main elements: **phishing**, **reporting**, **password management** and **training**. The approach used recognized employees' skill level, respect employee time, recognize employee progress and motivate users.

   The methodology used is divide in five steps:

   (a) Create a master list of behaviours.

   (b) Prioritize behaviours: considering how often the correlated incidents happen, which problems could cause, how much effort is needed to repair the possible issues.

   (c) Finding data, to find the related data sources to analyse and monitor the users' behaviour. For example, monitoring phishing is important control clicks on the link and gives data.

   (d) Define the success actions, what is defined as good user behaviour.

   (e) Chose a way to communicate with users, in this project is used icons a progress bar with dragons. Each dragon represents a different level of security, its comprehension is immediate for users 3.1.

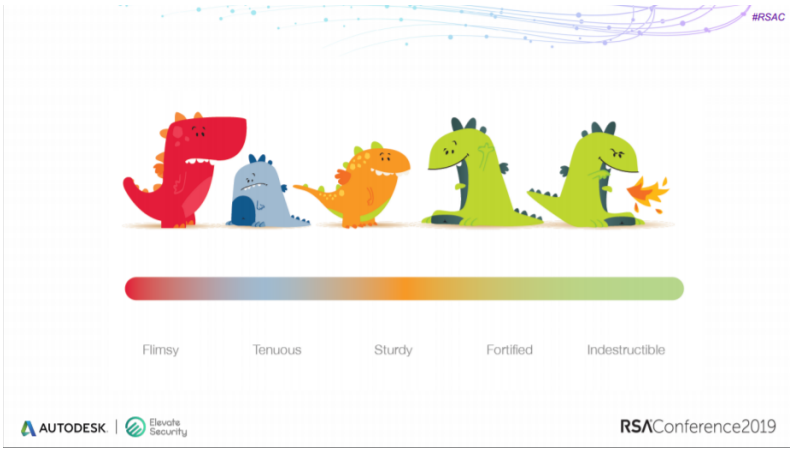

Figure 3.1. Progress bar in security snapshot (source: "Why Data-Driven Personalized Journeys Are the Future of Security Training").

The most relevant mechanics used are **progress bar** and **social proof**. The progress bar describes, in dynamically way, the user's security level. Social proof is defined as the

behaviour of people influenced by other peers, this mechanics is used to influence actions because other people already did the same things. Compare users with others: an individual with a team or department, increase the change of behaviour. The social proof theory is at the base of the e-commerce products comments, or social media mechanics. Communication is relevant, users understand in a clear way their security level thanks to an individual and dynamic score. The dashboard visualizes both the individual state of security in each subject (phishing, training, reporting, password manager) and the security level of departments and teams inside the company.

Results obtained by this project report interesting data related to time-saving:

- 445 hours saved cause employees do not need more training.
- 512 hours saved because users for the 69% recognize phishing attacks and avoid giving up their data.

4. Also **storytelling** is often successfully used as a game element to explain cyber security concepts. There exist some applications that, with the help of storytelling, assist users to better understand laws and more in detail referring to the comprehension of data protection regulations (es: GDPR) [70].

   The use of storytelling helps in converting ideas into concepts. The structure of storytelling is usually composed of four elements, following the structure of "Little red riding hood":

   (a) Characters' introduction and background of the story.

   (b) Begin of a problem and complications called trigger and incident.

   (c) The characters try to solve the problem presented with the resolution.

   (d) Conclusion.

   Some design elements important to keep in consideration when storytelling is used:

   - Thematic areas covered: it is important to present the correct vocabulary, in this case, referred to data protection, and teach this with understandable words for the target referred.
   - Chose the target: in this case, the user should have little or no knowledge of the subject.
   - Chose story structure: each module follows a uniform structure.

   Another example of the use of storytelling is given thanks to the ThinkData.ch case. It is an interactive service that provides information about data protection and transparency in an organizational context. It gives concrete examples and legal references thanks to the use of storytelling [71].

   As explained before, also in this case to build the story is followed the method of "Little red riding hood".

   Users can read and collaborate to the collection of questions and answers. The story used should be real or invented, but they have to represent a plausible scenario, they can represent a happened anecdote but not directly attributable to the parties concerned.

   Experts consider the use of storytelling as a great element to create the correct awareness referred to cybersecurity topics. The narrative helps the brain to imagine and draw patterns and experiential models, the narrative gives meaning to abstract models, graphics and images.

   Its use can increase company culture referred to cybersecurity thanks to the user's participation and user perception. Inside an organization create the correct cyber security culture is essential to involve every employee in the process and in creating the correct sensibility to the topic.

   The use of storytelling should help in this way [72]:

   - Creation of a tradition: to create a correct link between past present and future. In this way is possible to create a sense of loyalty and belonging.

Figure 3.2. Storytelling example referred to collect the biometric fingerprints (source: ThinkData.ch).

- Introduction of new elements: the story helps the introduction of new workers within the company.
- Story of positive and negative experience with the possibility of sharing experiences and skills, this element should decrease the number of mistakes.
- Narration of real story happened inside the company to increase the sense of responsibility.
- Increase communication at all levels, thus increasing the chances of a real understanding by workers with respect to IT security and its best practices, in relation to the roles covered and responsibilities.

5. Some applications of gamification in cybersecurity awareness use **video game** structure. In the program [73] ten employees, favourable to participate, are trained about password, social engineering, phishing and ransomware topics.

   The participation consists of three steps for the users:

   - Pre-game questionnaire
   - Play the game
   - Post-game questionnaire

   In the end, the instructor compares the results of pre and post-game surveys.

   The game was structured with precise workflow for each session, and with assigned points for each answer: 5 points for correct answers, 3 points for semi-correct answers and 0 points for incorrect answers. The result of this experience reports an increase of 51% of better knowledge in each category with a better result for the password and phishing section. Moreover, the users report satisfaction and more engagement than transitional training on the same topics.

6. Another interesting example is related to the **manufacturing system**, in this field the security choices are not trivial since they can affect the productivity of the company [74]. For this reason, it was created a game-based attack and defence mathematical model. The game has the aim to invite the user to reflect on attacks probability, probability of defence, strategy available for attack defence, the effectiveness of the chosen elements, cost of maintaining and implementing the elements chosen and cost of recovery. This application presents mathematical problems that should be summarized as search for minima and maxima, depending on whether you are playing as attackers or defenders, of the formula proposed.

   It is interesting to notice that this application keeps into consideration costs in different mining:

- Cost of implementation and maintaining the adopted strategy.
- Cost of recovery.
- Cost of production-related to the attack suffered by the company.

For the users is also possible to understand and think about the probability of attacks and the exposure created and therefore act consequentially.

7. Riskio is a serious game for awareness and education in cybersecurity created both for companies' environment and universities [75]. The aims of the game are:

   - Know vulnerability and attacks methods.
   - Know usable countermeasure.
   - Given the opportunity to users to make practice.
   - Reflect on the possible consequences.
   - Create a flexible game adaptable to a new context.
   - Easy to learn and play.

   It uses constructivism didactic method based on four principles:

   (a) Simulated authentic learning, the game board used represent a possible real scenario.

   (b) Active learning, riskio use role game, its aim is the mind-train user both on attacks and defence side.

   (c) Collaborative learning, players can interact with each other in order to create new knowledge.

   (d) Interactive teaching, the teacher gives feedback and correction, but he does not create a real lecture. He guides the discussion to lead students to the learning goal leaving them free to explore and confront each other.

   The game consists in a game board that represents a physical office with online services and card decks:

   - Attack, organized in different attack/vulnerability categories (Spoofing, Tampering, Non-Repudiation, Information Disclosure, DOS, Elevation of Privilege).
   - Defence, options of possible defence solutions.
   - Information, used by the master game to create and introduce new dynamics and elements of difficulty.

   During each session of the game the players take turns playing the role of attacker and the other ones play the role of defence. The attacker, using the attack deck, chooses an attack and describes it. The defenders present their solution to replay the attacks proposed. The master guides the game and he can use the information card to change and make more difficult the situation presented.

   In order to analyse evaluate the game, it was used the TAM method that evaluates, with a survey, the perception of ease of use, perception of usefulness, the intention of use. The results report that users perceive it more useful in the work environment rather than in the school system. The user reports an increased interest in the user of the game in order to perceive risk inside their organization.

   The game makes also possible the award of points to the various players according to the choices made, but this game element was not evaluated as interesting for the users. This distracts from the main goal.

3.2.2 School Environment

Other applications of cyber security education are tested in school settings, more specifically in high schools and universities.

1. In order to teach concepts and technologies related to cyber security, it was created a game in a university course. Standard lectures are extended with the use of a gamification platform, students are free to choose if participate and use the platform or follow only the standard course [20]. The choice, being free, has no impact on the final vote. The metaphor is the principal element used in this experiment. It is used to represent the technical concepts. For example, to represent the brute force attack the avatar has to try all the available keys to open a door. The model used is based on **perceived usefulness**, students perceive that the game helps the learning phase, and **confidence**, recognition of the professor as an expert and therefore the assumption that the knowledges acquired are true and correct.

   Results report that students who use the game complete both the assignments present during the course for the 88% respect the 38% of students that do not use the gamified system. A relevant result is related to the dropping-out trend: the 57% of students that do not participate in the game drop out. This number is important and can represent a factor to pay attention to. If the user voluntarily decides not to participate in the program with gamification it is possible to recognize a range of higher risks. People that do not participate, although they have the possibility to study anyway, fail with a higher probability. The dropping out rate should be caused either for a low initial level of interest or for losing interest during the semester. Could be interesting to understand and analyse the actual reasons with the purpose to concentrate also on this target. In general, should be useful to recognize different risk levels in relationship with the use of the gamified system, however the previous study reports only a greater degree of failure in those who decide not to participate in gamification at all.

2. Thanks to the study [76] was theorized the relationship between **time on task** and **leader-board**. Based on gamification learning theory, this project tries to motivate students to work on their final project a little at a time and encourages them to not leave all the work for the last moment. To do so they used a leader-board that exploits three game elements:

   - Conflict and Challenge: competition between peers, every student has the same possibility to appear on the leader-board. This aspect maximizes the impact on time on task.
   - Rules and Goals: a clear expression of who will be displayed on the leader-board in relation to which results are obtained. In this context, the metric used to evaluate was the speed of execution of a task. For the user, the goal must be clear, measurable and feasible.
   - Assessment: the method used to express the improvements in the game.

   The study was performed in this way: each student has to develop a final project before the end of the course. Many students used to complete the project in the last available days with a drastic decrease of the time devoted to it. Consequently, also the accuracy and the final grade were also affected. In order to increase the time during the semester spent on the project, professors create a leader-board organized into specific tasks: the first three students that complete the task were marked on the leader-board. Even if the final grade does not consider the presence or absence in the board, the relation between time on task and leader-board is confirmed by the greater result obtained by the students that used the leader-board respect the standard class.

   An observation related to this project is that the leader-board used is static for each task, is not possible to earn or lose positions for one task once the three winners were awarded. The effect on a dynamic leader-board is more complex to organize mostly to give to all users the same possibility to appear during all the semester.

3. Interesting results are obtained by an Italian project [77] performed in high school settings. It was performed to increase the consciousness about cyber security using gamified elements.

It was interesting to note that students well-disposed to change their behaviour belong to schools with poor computer training in contrast with the school with a greater computer learning program like technical college. This tread may mean two things:

- Students with more technical notions already adopt secure behaviour because more conscious.
- Students that recognize the computer environment as familiar are more relaxed in the use and so perceive risks in a distorted way.

This study is also interesting for the target, high school students represent a great portion of users that every day use the internet and the computer world without real education.

4. In the education environment competition like **CTF** could also be seen as gamification. An example is reported by [78]. In this example the competition is divided into four levels:

   - Basic programming information.
   - Web application (XSS, SQL injection).
   - Application security level (binary exploitation, buffer overflow).
   - Reverse engineering, forensic concepts.

   Each team has access to an OVF image for virtual box, the game server monitors the team's flags and the available services. It uses a public scoreboard both for the attack and defence results for each team. This technique is useful for students to apply in a practical way knowledge often learned only theoretically in a real but protected context. The principal limitations are represented by previous technical knowledge needed for the participant, for that reason a CTF can be used only in a specific context. Another limitation is the time: usually, a CTF lasts one or two days, this aspect is in contrast with the gamification idea that needs a long used period (more than one mouth) to give benefits.

5. Always related to CTF, the University of Padova organized its course on Mobile Security [1] using CTF. The course was organized with challenges, assignments and a leader board. The topics covered by the challenges were: app development, reverse engineering and exploitation. The challenges follow a structure similar to CTF organization. The student final result takes into account 40% of participation and outcome in the challenges [79].

6. Instead, the University of Czech Republic proposed a gamification application in cybersecurity education [80]. This application differs from others because students are called to create a serious game about security, instead of learning by playing. The idea is to educate future technique experts about security to make up for the lack of professional figures in the environment in anticipation of the numerous job vacancies.

   The project use KYPO cyber range as tool to emulate real attacks in a controlled environment [81]. The organization of the course was structured by following guidelines about defence, threats, network, attacks and penetration tests. In addition to the theoretical concept, the courses are organized as cooperative learning and project-based.

   The university proposed two courses that follow this direction, the first preparatory to the second one:

   - Cyber Attack Simulation (Introductory). During this course, students follow both theoretical lectures and practical experience. During the practical experience student, in little groups, have to create a game. The serious game created by students should be presented during a University Open Day.
   - Cyber Defence Tutorial (Follow-up). Students, autonomously, have to create a gamified experience based on the service chosen by the student himself. During this course, theoretical information is not provided, because it is assumed that the student already has the basic knowledge required or the tools to obtain the desired information. Also in this case, the game created is presented during the Open Day.

[1] For this element I thank Marco Casagrande, teaching assistant for the course "Mobile Security and IoT" at the University of Padova, for letting me know about the project.

In this project an essential element of gamification is represented by feedback:

- In-class presentation: possibility to compare the project elements with professors and peers.
- In-class consultation: private consultant with professors.
- Test-ran: possibility to compare the work with external security experts.
- Open day: presentation of the work to other students and real use of the game by others.
- Final Project review: comparison with the professor for the final evaluation.

This application underlines two possible use of gamification in cybersecurity:

- **Game creation**: students interested in technical cybersecurity and computer science knowledge have to use specific skills to design, create and manage the game.
- **Game use**: during the open day new students can learn cybersecurity concepts thanks to the work of other peers and be interested in the subject raising awareness.

7. Another use of gamification in security education is related to the **risk for children and young people** on the internet [82]. Teaching the children, the correct use of devices could help also them to be aware of cyberbullying, cyber grooming and illegal interaction. The experience create, in this case, has the aim to limit and avoid illegal content, harmful content, inappropriate content for the youngest users and privacy related problems as identity theft, personal data exposure and oversharing.

   The gamified experience involves teachers, parents and children. In this case, the use of gamification tries to avoid both incorrect uses of devices creating a correct education and preventing psychological issues potentially created by cyberbullying or similar events. The game elements used are points, social interaction and social comparison using both collaboration and competition.

3.2.3 Private use

Other applications of gamification are possible to find in a private environment, in the sense that user interest in the subject can interact with systems and projects freely thank their interest and not in a specific external context.

1. Tanks to the cybersecurity European month, Google and Euroconsumers created a game named Space Shelter. This game is free to use and it was created to help people of all ages with cybersecurity topics [21]. It is set in space, the gamer needs to answer correctly the questions proposed in order to get to the international space station. It takes ten minutes to complete and it is a quiz game.

   The topics presented are:

   - Password: how to create a secure password, password manager, wrong habits related to the password usage.
   - Two factor authentication.
   - Phishing: what it is, what elements to pay attention to recognize phishing messages.

   In addition to the game itself, there were planned two different activities for different audiences [83]:

   - For the non-profit organizations, three free webinars are planned about privacy, phishing and cyber scams. These meetings are free for everyone but designed primarily for non-profit organizations. The goal is to increase awareness and competence also in a not productive sector.

- For teenagers, thanks to the collaboration of YouTubers and the astronaut Paolo Nespoli are planned two videos. Thanks to the use of storytelling and social influence, users are encouraged to try the game with the purpose to increase cybersecurity awareness in the younger generations.

2. Always related to the private environment, but dedicated to cybersecurity enthusiastic there is the world of CTF. There exist competitions during which users, regardless of education or company environment, can challenge each other about cyber security technique topics.

   Similar to the CTF is the platform contract teach to the users ethical hacker, hacking techniques and it can also work as training for CTF competition. Online different platforms allow users, with an initial interest in the subject, to study and apply their knowledge about cyber security in a protected environment. These types of platforms are dedicated to users with a technical interest in the subject, both for experts and beginners.

   For example, the platform Try Hack Me, after the registration, asks the user for his starting level: Beginner, Early Intermediate, Intermediate and Advanced and why he would like to start to learn cybersecurity. Once selected the preferences, the player can start to learn. The learning phase is organized by real-world labs. The platform aims to make it more accessible and easier to practice cyber security [84]. Inside the platform are used some game mechanics and dynamics to motivate users inside the player journey like points, level and leader board, but it is clear that the first motivator factor is a personal interest.

3. A recent example of storytelling was used by ECSM for the cybersecurity 2021 month [85]. Inside the campaign "Think Before You Click #ThinkB4UClick", there have been told two little stories related to real cases of attack. In the first story, a woman talks about her experience with a phishing attack followed by ransomware that blocked its social media profile. In the second story, a boy explains the risk to share his own device with others, also if he trusted them. Both stories are organized in three little videos during with the protagonist tells how the attacks have happened and how he or she recognize to be under attack, how they felt and witch actions they did. In the end, they give tips to avoid the same mistakes and how easy it was to fall into the scam.

   This type of narration is useful to bring the thought of the community closer to security, especially about banal actions carried out daily.

4. Other types of applications of gamification in cybersecurity are represented by **board game**, some examples are summarized here:

   - Kaspersky Industrial Protection Simulation (KIPS) [86]. Users have to protect company information and communications. They have limited time and resources to use in order to make the correct decision. These elements want to reproduce a pressure test and recreate the mood of a stressful environment during real attacks.
   - d0x3d! [87]. It is a board game to teach students network and security elements. Students have to follow the network algorithms to simulate the steps usually done by devices. As game elements, this game is concentrated on collaboration between classmates.
   - Control-Alt-Hack [88]. It is a card game developed for primary and secondary schools in order to create the correct attitude for computer science subjects.
   - Elevation of Privilege [89]. Card game for developer and computer science experts, the aim of the game is to increase cybersecurity knowledge in computer science environment.

5. As the last type of gamified experience, it is possible to find **scavenger hunt**. The Scavenger Hunt should be organized differently with concrete implementation, web-based or mixed one, but in general, users must be able to obtain all the information they want thanks to clues.

   In this experience, [90] was used Gather in order to recreate a scenario similar to work at home used to provide information about security at home. The use of this technique is more used for not expert and start to create sensibility about the subjects [91]. For this reason, many of these applications are created during the Cyber security month in October.

However, it is possible also to find some applications for more experts or interested in [92]. This is Cyber Scavenger Hunt, which is an interactive website used to start thinking like a penetration tester. The experience is organized into 8 steps, and for each step is possible to ask for three hints that help the user to obtain information and discover new elements.

3.3 Serious-Game and Gamification Cybersecurity Framework

In this section are summarized frameworks and guidelines for cyber security with the purpose to analyse existing literature and generalising the approach for gamification in the next chapters. In the following subsections, it is possible to find both frameworks related to gamification and serious game. In the literature, it is very hard to find frameworks directly related only to gamification for cybersecurity, but it is more common to find cybersecurity serious game frameworks. As previously mentioned, the analysis of serious games and their applications differ slightly from the objective of this thesis, however, their analyses should be used to generalise the approach also for gamification purposes.

3.3.1 Designing Cybersecurity Serious Games

The project [93] organize and summarize serious game design elements by proposing a methodology. The scope considered is the training of future IT security experts. The methodology is organized in different points:

- Learning Objectives: the contents must be organized logically distinguished in areas, units and arguments. For the choice of content, it is necessary to follow guidelines official.
- Challenge design: the content must be based on the learning objectives previous selected. It is possible to design the challenges following a real attack life cycle (Initial compromise, Establishing Foothold, Privilege escalation, Internal Reconnaissance, Lateral Movement, Maintaining Presence, Completing the Mission). It is preferred to present the security problem rider than concentrate the attention on specific tools or programming languages. It is needed to manage the challenges levels progressively and avoid waste of time.
- Rules: clear definition of rules, specification of denied actions and countermeasures adopted. hints: use of hints and help to avoid users' frustration and blocking challenges. It is possible to use game mechanics to active hits, for example, use virtual points or coins.
- Game elements:
  1. Narration: use the story as an accompaniment to the user during the game. It is possible to reflect the information known during an attack depending on the phase in which you are. It is suggested to use a brief story with a focus on important aspects to avoid boredom and distraction.
  2. Injects, use notifications, messages, warnings in order to keep users' attention, time pressure and inform users about technical problems.
  3. Player identity, create an identity for the player for example using an avatar, in which users can personalize themselves.
  4. Rewards: recognize the user outcome with badges or points visible to other users.
- Technical Aspects: chose the technical aspect needed for the experience (for example virtual machine).
- Testing: a key step is presented to test every aspect more than once before the official run.
- Data gathering and privacy: choose and implement elements to gather data needed to evaluate and control the project. However, it is important to keep into consideration the privacy issues and the GDPR policy. it is possible to use surveys pre and post-experience in order to collect feedback on the project.

- Evaluation: evaluating the project based on event logs, user perception and observation.

3.3.2 COFELET

The Conceptual Framework for Developing Cyber Security Serious Games (COFELET) [94] [95] is a game-based approach for the design of computer security teaching programs for future new experts. The aim is to create an educational program motivated and "always-on". The passive activities are reduced to the minimum with the purpose to increase practice competence and active experiences. With the idea of continuous learning, it is possible to work both on new experiences and challenges and the user can learn the same things from other points of view.

The framework it is based on:

- LM-GM framework in order to select the game mechanics [45].
- CAPEC, dictionary attacks patters [96].
- CKC, model that organizes the cyber attacks in phases [97].
- NCWF, the definition of rules, knowledge, skills necessary in a cybersecurity scenario also referred to the user's roles considered [98].

The model, graphically represented in the figure 3.3, it is composed of different elements, the most important are:

- Task: actions done by users or instruction inside the game.
- Goal: problem that the user must solve in the game.
- Condition: pre-requirement needs to solve the task.
- Scenario execution flow (SEF), steps needed to solve the task (one task can have one or more SEF).
- Education context: characteristics of the environment in which the game will take place.
- Gaming context: game elements (points, durations, avatar etc.).
- Scenario: internal narration that includes level structure and missions.
- Knowledge skills ability (KSA), skills needed to the user during the experience based on NCWF definitions.
- Learning objects: elements that we expect the player to have acquired at the end of the game session.
- Teaching content: material used for educational purposes (text, videos etc.).

The learning level is organized thanks to the Bloom theory distinguishing in Remember, Understand, apply, analyse, evaluate and create. At the end of the session, the user is evaluated thanks to performance measurements and the user receives feedback.

There exist different extensions of the model [99]. One it is created with a particular concentration on attack patterns, with learning content refereed to methods, techniques for future experts in the sector.

In order to organize the primary element, it uses a quintuple schema organized with:

```
<entity, property, property value, source, destination>
```

For example,

```
<port scanner, sends, icmp type 8 packets, player host, network>
```

This structure should be used to organize the experiences and the flow keeping into consideration the next steps and conditions.

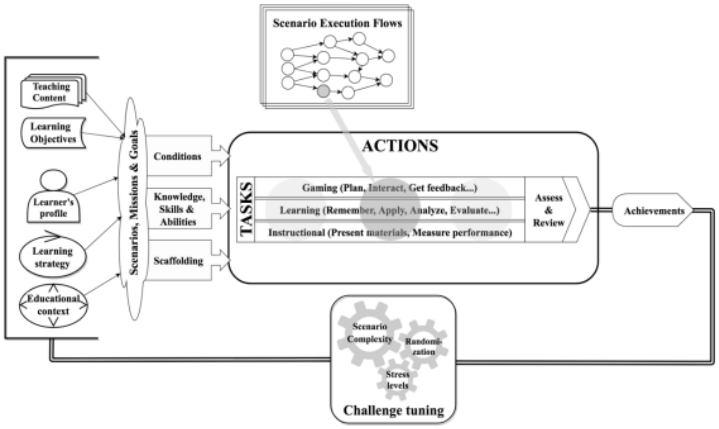

Figure 3.3. COFELET model (source: "Conceptual Framework for Developing Cyber Security Serious Games").

3.3.3 CybAR

The project [100] used augmented reality in a game for cybersecurity. The topics considered are spoofed emails, SMS phishing, scamp phone calls, theft of identity, ransomware, phishing on social networks, spam, mobile security and public wi-fi.

The work proposed a model used to design and organize the learning object inside the game. The model is composed of some elements:

1. Perceived Susceptibility: the subjective probability of the user that an attack affects him. Each activity displayed in the game is associated with a potential cyber security threat that appears as a case during the experience. The player's job is to perform the tasks properly; each execution of activities is followed by immediate positive or negative responses. This game design faces user awareness of susceptibility to the threat to cybersecurity.
2. Perceived Severity: it is the perception of negative consequences. Within the game, every wrong choice leads to countermeasures proportionally to the error made to raise awareness of the severity of the threat.
3. Perceived Threat: threat perception as dangerous or negative. It shows the harmful consequences following the attack so the user can reflect the consequences.
4. Perceived Safeguard Effectiveness: in the game, if the player does not know how to recognize the problem can receive help/ advice and thanks to feedback know how to recognize the problem later to identify attacks.
5. Perceived Safeguard Cost: perception of the costs related to an attack seen from different points of view: physical, cognitive, time, money, discomfort, recovery and threat recognition.
6. Self-Efficacy: confidence in themselves and in who takes the measures presented. The game provides information in order to create self-sufficiency in recognizing potentially harmful situations.

In the figure 3.4 it is possible to see how each element interacts with others in order to change behaviour about cybersecurity threats.

3.3.4 Cybersecurity Awareness Framework for Academia

This project creates an education program about computer security, especially to face the increasingly numerous attacks that target people. The program is designed for high school students in

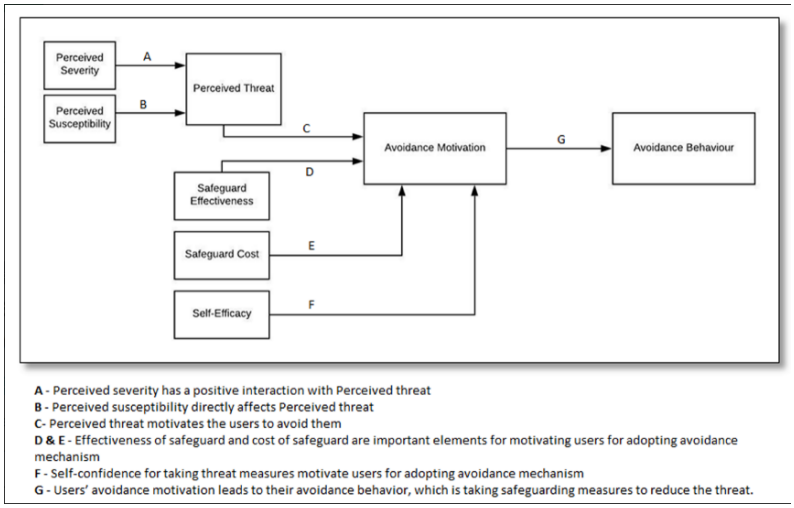

Figure 3.4. cybAR framework (source: "Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness (CybAR)").

order to face both the scarcity of training programmes in schools and the low level of general knowledge [101].

The program is based on creating a participation culture on cyber problems in the community, clear communication, clear evaluation based on attacks and defence results, regular updates, continuous training, repetition of the content, creating progress reports and include gamification.

The CAFA (Cybersecurity Awareness Framework for Academia) framework is composed of two main elements:

- ICTS (Information and Communication Technology Support): technical organization on the management of LMS and support for the design of training modules.
- CAC (Cyber Security Awareness Centre): search for the latest updates and best practices to keep your system up to date related to cybersecurity topics.

In particular, the project proposed four courses of security, one for each high school year called CATM-0/1/2/3. The aim is to encapsulate the new trends/attacks within the security program into modules, populate each module with directions to the type of questions and gamification to be used, analyse the results for each module proposed for continuous improvement.

- CATM-0: an introductory course for new students, the content items are defined based on topics and competence chosen by instructors.
- CATM-x (1/2/3): a course in other years of high school. In these courses, it is possible to distinguish between two subsections.
  - CATM-xg: that is general, referred to a specific moment of education related to cybersecurity.
  - CATM-xs: it is a specific course and security training taught in a transversal way during other subjects such as English, Mathematics. This should lead students to understand safety as a multidisciplinary element.

The use of gamification is directly included in the framework, but it is not specified how to choose game elements and design gamification experience.

3.3.5 e-ADR

The project [102] is created to teach not IT experts about security information, more in detail about incident detection and handling. The content of the experience is focused on malware and password management.

The model proposed by the e-ADR approach is graphically represented in the figure 3.5.

The model is composed of four steps:

- Diagnosis
- Design
- Implementation
- Evaluation

Each step is internally divided into five elements:

- Problem formulation (P)
- Artefact creation (A)
- Evaluation (E)
- Reflection (R)
- Learning (L)

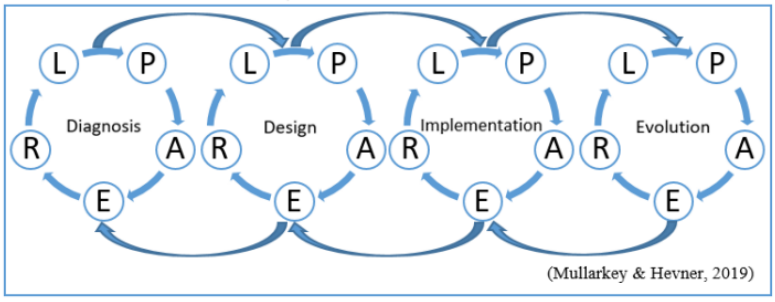

Figure 3.5. e-ADR model (source: "An e-ADR (elaborated Action Design Research) Approach Towards Game based Learning in Cybersecurity Incident Detection and Handling").

What is interesting for our purposes, is that the framework directly allows a continuous iteration and improvement both inside each step and across the model.

For example, the project was performed three iterations on all the models. During the first one, the cybersecurity content and game objects were defined. It was established the correct action sequences were in case of the incident using NIST guidelines. They receive feedback from experts about improvements. In the second iteration, the learning content was improved, and user engagement was included thanks to the feedback received in the first iteration. In the third iteration, it was created a real implementation in a real-time office environment. This aspect of continuous improvement should be used to face both continuous learning and training models and continuous updates.

After the experienced users are evaluated focused on user reaction during the experience, user learning, user' use of new knowledge and skills and user learning outcome. Also, this aspect is interesting to create metrics and evaluate all the experiences.

3.4 Open Issues

3.4.1 Development and Design Choices

The theoretical study and the real application of gamification in the cyber security field do not report clearly and systematically how to choose the **game elements**. Except for the leader-board related to time on task and knowledge acquisition in the school environment [76], it is not specified the actual interaction with the elements for the users.

There are some specifications for elements preferred on the base of the users' topology because the gamification elements are linked with motivators. However, each research that puts in relation to motivation and gamification elements are done by experts and rarely considers users opinion and experience. Moreover, the relations and the results obtained by the game elements interaction and correlation are not analysed.

All the reported gamification applications in cyber security do not follow a specific **methodology** or framework. Often, they are based on gamification theories, but each implementation follows a specific design process. In the previous section are presented some of the most know frameworks that should be applied in every environment, however the adaptation of these in the cyber security fields is not easy and needs additional elements not yet well theorized.

3.4.2 Privacy

An important aspect to keep in consideration is the privacy [103]. Privacy requirements should be:

- Anonymity: the user is not identifiable by other customers.
- Pseudonymity: use of pseudonyms, instead of the real name, to avoid recognition.
- Unlinkability: impossibility by third parties to create relationships between subjects and actions.
- Undetectability: recognition of the existence of one component is not possible from third parties.
- Unobservability: possibility to hide users' actions.

There are some game design elements recognized as dangerous for privacy thanks to its intrinsic features like avatar, challenges, communication between users and competitions. On the other hand, other elements are safe for their nature like time, badges, rewards. The user control as points, competitions and leader-boards can create large amounts of user's related data. Many gamification programs do not consider and protect privacy also if it is used inside a closed group like a school or company. This study proposed a schema to take into account starting from the beginning phase of development following the concept related to "privacy by design" 3.6. Considering the GDPR the privacy and data processing concepts are not negligible.

3.4.3 Ethical Problem

Another problem that arises is the ethical reference related to the self-determination employees' capability [104]. The basic idea is that the gamification technique inducts users to change their behaviour and obtain a "spontaneously" new practice and habits without any external impositions. Thanks to gamification, the game dimension and the work dimension are linked, one risk is that the worker loses self-determination and freedom. The analysis reports the fear that companies ask the employee to give more than their real physical and psychological attitude. There are reported four main ethical issues:

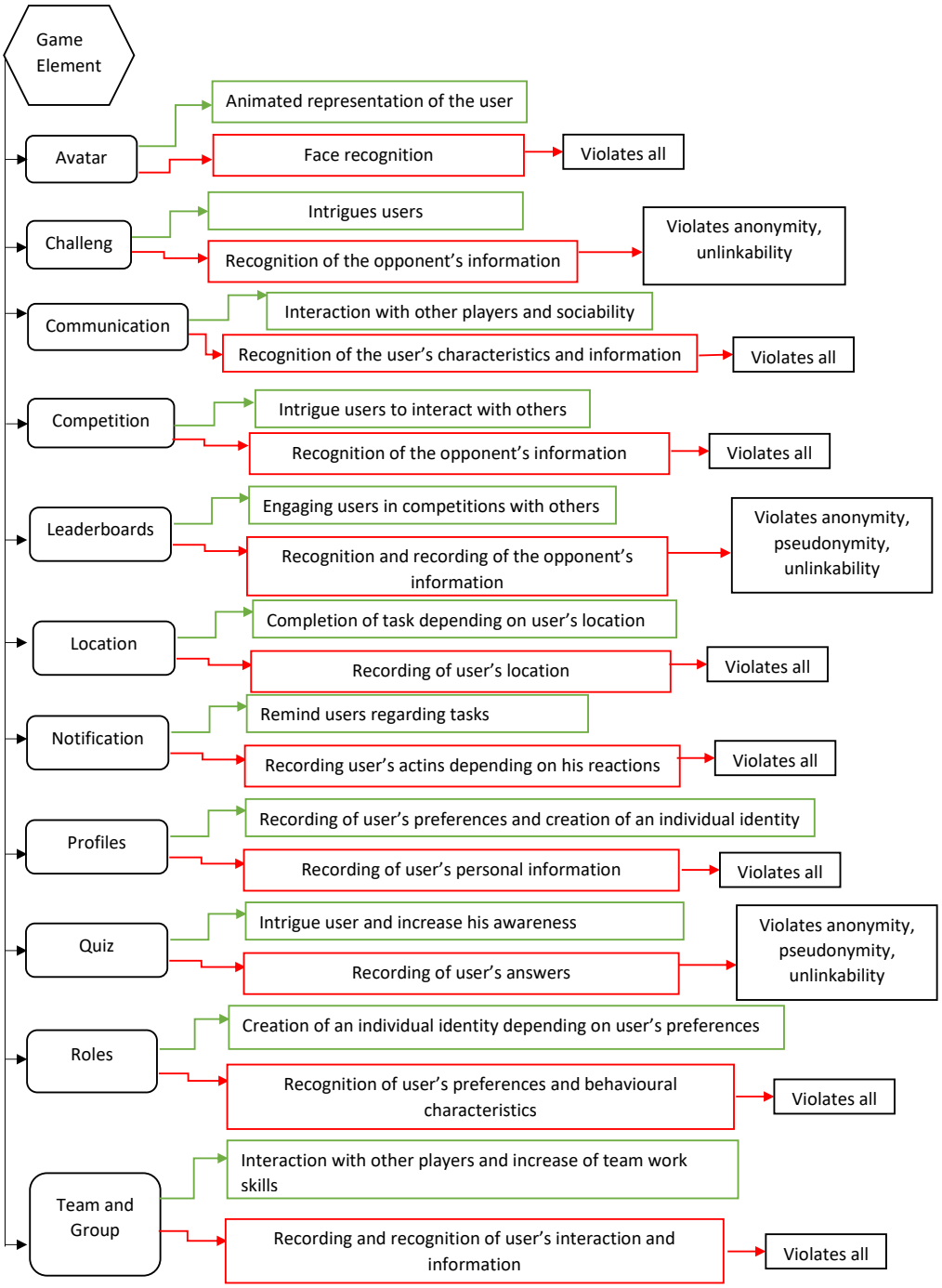

Figure 3.6. Privacy schema (source: "Gamification vs. Privacy: Identifying and Analysing the Major Concerns").

- Exploitation: player and provider relation in the real world is in imbalance, the provider should take advantage of players.

- Manipulation: in the real world player cannot make autonomous decisions. The provider forces the decision.
- Harm: If the gamification activity produces in the real world a physically or psychically injury.
- Character: if in the game the player in order to complete game objectives cannot respect human values.

Moreover, is important to keep into consideration the dependency factors, game elements work as cognitive doping. The new concept in companies is not substituting humans with machines, but using machines to encourage, motivate and persuade employees. So, it is essential to create a process safe and that the user perceives as trustable. Respect the user limits, attitudes and predisposition without force or manipulating their interaction is at the base of the user respect.

Chapter 4

Users and Experts ideas and suggestions

In order to create a useful methodology, we compare the ideas of users (also not experts in security fields), experts in gamification and cybersecurity and professor experiences with active learning in a university context.

4.1 User's perception

4.1.1 Survey

To analyse the thought of common users about cybersecurity we created a short questionnaire via Google Forms, and we shared it via the main social media (Facebook, Instagram, WhatsApp Contacts). We choose as target people with different experiences and different ages, especially not experts in cyber security environment with the purpose to collect their ideas, experiences and perceptions about a topic linked with security in computer science.

The idea of involving people that every day, both for work and personal business, is connected to the internet and use devices to communicate is important to reflect the security perception of the community. The survey would like to analyse how and when people were educated about cyber security topics, especially comparing active and passive education.

Another aim of the survey created was to retrieve information about how people live education in the work environment with the aim to recognize the limits and strengths.

The survey was formed by four sections:

- General user information as age, the environment of work or study and general security perceptions.
- Information about how they were formed about security (reserved for participants that already followed a course about cybersecurity).
- Introduction of game elements that they will prefer in a work environment used to create education about security.
- Conclusion, last comments and a free possibility to exchange contacts for future updates.

In general, thanks to the comments left by the interviewees, it denotes an interest in the subject often limited by the inability to train or defend themselves if they belong to the field of work/ study far from cybersecurity. It was recognized a general training is necessary for everyone, starting from the educational environment.

About 60 people expressed their interest in staying up to date on the subject and on the resource results.

The survey created, reported A, was written in Italian because shared with Italian users.

4.1.2 Who did participate to the survey?

The sample analysed consists of 206 participants. As shown by the graph 4.1 the participants are heterogeneous by age group, the only age range completely absent are the people under 18 years old. Also related to areas of study and work the survey results report a broad scenario.

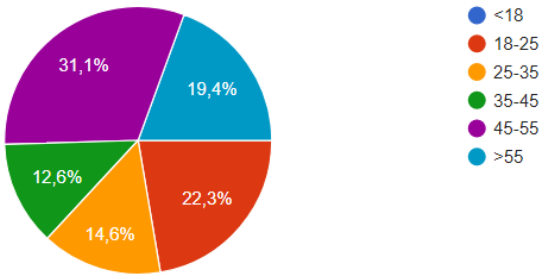

Figure 4.1. Participants to the survey by age group.

Here the sectors represented: commerce/marketing/economy, pharmacy/pharmaceutical technologies, chemistry, technical assistance, dance/music/entertainment disciplines, school (primary and secondary school teachers first and second grade)/education, arts/graphics/design and fashion, computer science, engineering, sport/ fitness and wellness, team leaders, consulting, unemployed/retired, architecture, nursing/health professions, health/medicine/dental, mental health, veterinary, agriculture, catering, languages, mechanics, geology, geography, insurance, craft, call centre, tourism environment and territory, disability, bank and road safety.

It is possible to group the fields of study and work in 4 main sectors: artistic, humanistic, technological and healthy. The disciplines are summarized in the table 4.1:

This variety both in age and in sectors of interest allowed a general approach to cyber security and not related to a specific environment.

4.1.3 Importance perception cybersecurity

As shown by the graph 4.2, about 73% of participants believe that cybersecurity is important and that it concerns themselves, 17% believe that it is important, but that they cannot act in person. 8.7% believe it is important but not for their own business. Only 0.5% believe it is not important. Then there are two specifications for which safety is considered important, but difficulties are expressed:

- Understanding.
- Defending themselves personally against company security, as in the last case there are filters and precautions managed by experts.

Considering the answers to the same question, but only for the trained participants, we can see a change of perception: 90% of the trained users replied that security is important and that concerns him personally, no one answered "No". A person does not think it is important for his activity and 4 interviewees do not believe they can act in person. This figure 4.3 is certainly relevant regarding the results of training in computer security. The results improve again if

Artistic disciplines	*Humanities disciplines*	*Technological disciplines*	*Healthy disciplines*
• Dance • Music • Spectacle • Graphics • Design • Fashion	• School • Team leader • Mental health • Languages • Tourism and territory • Disability	• Technical assistance • Computer science • Engineering • Consulting • Mechanical • Geology • Architecture • Craftsmanship • Call center • Marketing • Bank	• Medicine • Dental • Dental technician • Nursing • Health professions, • Pharmacy • Pharmaceutical technologies • Veterinarian

Table 4.1. Participant's work or study sectors

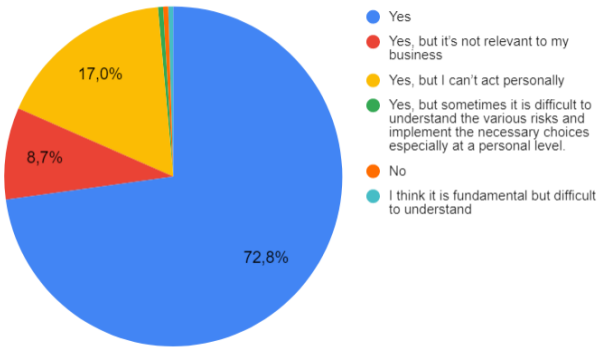

Figure 4.2. Participants to the survey importance perception.

only trained users with active training are considered: all participants, except one, consider cybersecurity as important and that concerns them personally. Only one participant considers it fundamental, but he does not believe that can act personally.

Therefore, it is clear that most of the participants feel the security important but many think to not be able to act in person. The training, in general, grows the security perception important and relevant for the people from 72% to 90%. An important aspect is that no one of the trained participants thinks that security is not important for themselves, even if they do not work in a computer science environment. Considering the trained people persist a little portion that does not know how to act practically. It is possible to notice that this number decrease if the people are trained with active education. So, it seems clear that to increase the user perception and awareness training is needed and active trained is preferred to give a robust consideration of cybersecurity also referred to the ability of the people to act personally. It is also true that most of the people that followed an active training work in a computer science environment, not directly related to security, but it is very likely that they already have a sensibility and personal interest in the subjects.

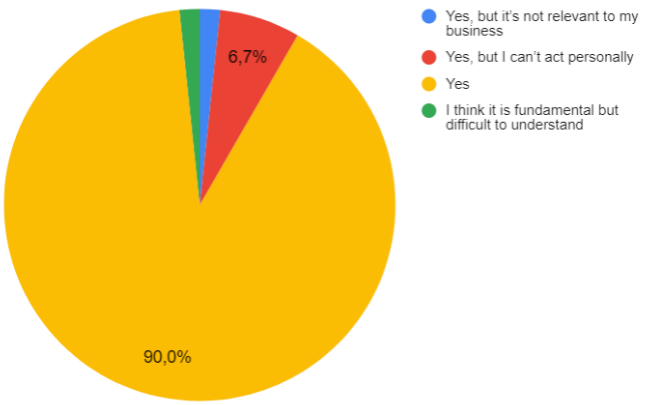

Figure 4.3. Importance perception for the trained users.

In order to analyse the different perception related to cyber security for age range, is possible to notice the graph 4.4 that report the comparison between the number of total participators for age range and the number of users that consider cyber security not important or relevant for themselves.

Considering the proportion between the number of participants per age range and users security perception different from important by age range, the age group that most recognizes cybersecurity as important is 45-55. Followed by the band 18-25 and 25-35. Instead, it seems that the less sensitive to the topic is the band of age 35-45.

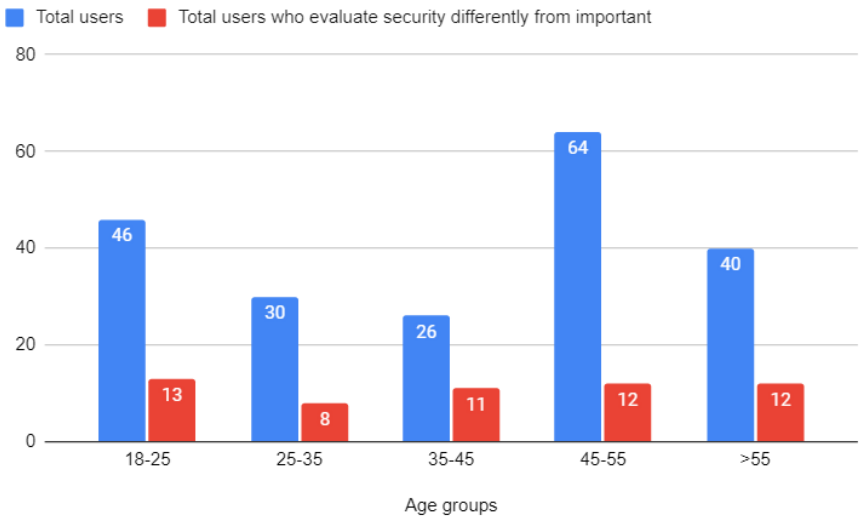

Figure 4.4. Security important perception by age range

4.1.4 Training

Compared to the total sample, 70.9% said they had never taken a course on cyber security, however, 60 people (about 30%) have attended at least one training course. This element proves that in our society safe training related to computers is not yet considered a key element and is not managed on a large scale.

The areas of work and study most sensitive to the subject are those of school/education (16 in total), disciplines directly related to computer science (11) and call centre (2). Instead, the

active training is mainly used to teach cyber security directly linked with the computers and technology topics (network security, engineering, ICT, computer science, consultant, information technology), then is also possible to find some participants from the pharmaceutical environment. Therefore, it is possible to notice a correlation between the field of interest or work and education in cybersecurity both for the method chosen during the learning phase.

Only considering the 60 participants trained, 73% followed a mainly passive training while only 27% followed active training (interactive videos, game-like experiences, simulations). As shown in the figure 4.5, the completely remotely training course is the most widely used, followed by use completely in presence. Intermediate solutions are rarely adopted (7 participants in total, about 12% of the sample).

So, it is possible to deduct that the preferred training style for the companies is a passive and remote training. Only for the discipline strictly related to computer subject, the active training is preferred.

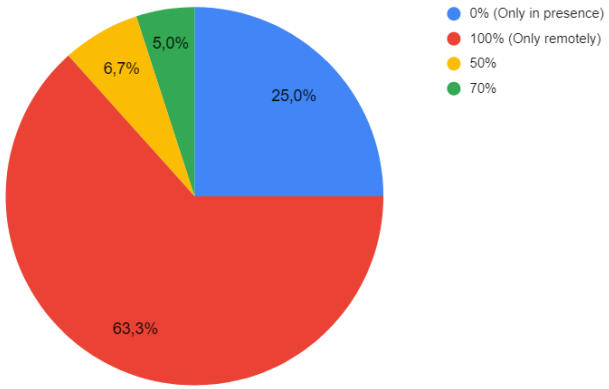

Figure 4.5. Remote or in presence course fruition

Only 5% said they had a fully organized course with **group activities**, compared to 81.7% who said they had no group activities. Also considering only the users with active training only 12% followed a course fully organized with group activities and only 3 users have been trained with group activities of intermediate duration. Therefore, the organization of the course with group activity appears to be rare both for active and passive training. This element shows a difficulty to organize group training in the work environment.

For 17 interviewees with active training, their results during the course were summarized in **points**, and of these 9 users score was compared with the results of other colleges. It is possible to notice that the use of points is common in showing the results obtained during active training because all the users that followed an active training report the points as a measure of their work. But, at the same time, is not so common the comparison with other colleges results. It is possible that this choice is made to avoid competition and frustration in the user, but it is interesting to recognize the points as an almost unique method of evaluation and comparison.

For the **frequency of training/update courses**, 43% of the training courses were followed only once, 35% once a year and only 15% several times a year. A person emphasizes the fact to follow updated courses on the subject only if it is mandatory by the company. It is possible to deduct that the courses are followed at once in the onboarding phase in the company for most cases or only once during all work experience. But in general, it is clear that the course is enjoyed as a unique element a not like a process as continuous education. Only for very few users, the training is not a task to complete once or twice a year (or less).

The main **difficulties** encountered are "Difficulties in understanding how to act actively for personal and corporate security", "Difficulties in implementing the advice received". And then (8 preferences) "Difficulty in understanding abstract and theoretical contents". However, about 48% of the participants said they had no difficulties.

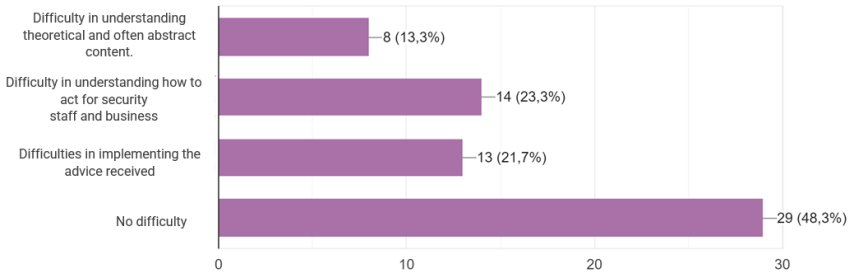

Figure 4.6. Difficulties encountered

Comparing the **difficulties encountered in training for users with active training (16 participants 4.7) and with passive training (44 participants 4.8)** it can be noted that: with active training about 70% did not encounter any difficulties. As for users with passive training, only 37% said they had no difficulties, while 27% said they had difficulties in understanding how to act actively and 22.9% difficulty in putting into practice the advice received. These last values are interesting if compared with the graph related to active training: only 6.3% declare to have difficulties in understanding how to act and 12% to have difficulties in putting into practice the advice received.

However, referred to theoretical concepts, the difficulty is equal to 12.5% for both types of training.

These data report that using an active formation drastically reduces the number of problems and difficulties encountered usually during formation about cybersecurity. Creating an education clearer and more compensable is the goal of the training and awareness process, especially both in understanding the concepts and in knowing how to act correctly in case of need.

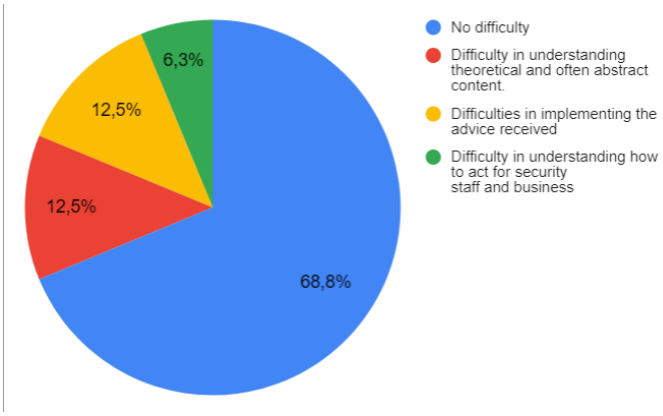

Figure 4.7. Difficulty for users with active training

Considering **the perception of users regarding the usefulness of training**, about 62% said they were interested in it and found the training useful. 12 users, despite their initial interest, do not know how to apply the acquired knowledge. 4 users were not interested. Instead, 7 users, initially not interesting, have perceived the utility.

Comparing the results with the **usefulness between formats actively 4.10 and passively 4.9** by the graphs we can see that for active training 75% were interested and are satisfied with the work done, 18% were interested, but they do not know how to apply the acquired knowledge and 6% were not interested, but they perceived its importance.

On the other hand, with passive training 57% are satisfied with the work done, about 13% changed their opinion about it during the training recognizing its effectiveness, 16% do not know

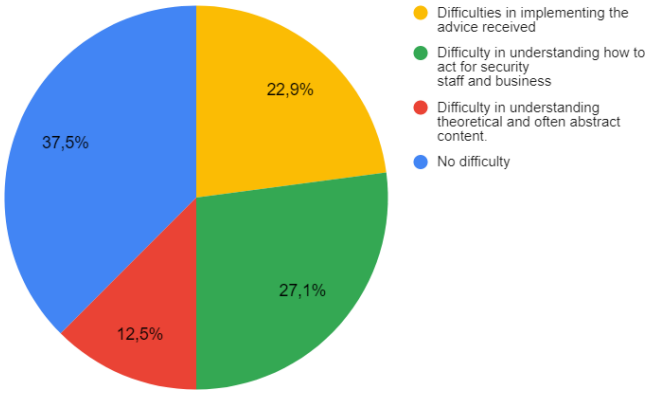

Figure 4.8. Difficulty for users with passive training

how to apply the knowledge received to which can be added a 9% who recognized the training as useless and two users found that the course, as it was organized, was not useful.

It seems that active training creates a better perception of training usefulness compared to passive training. On the other hand, with passive training the number of users that recognize the course as useless grows. It is important to notice that no users with active training consider the followed course as a waste of time compared with the 9% of the user with passive training.

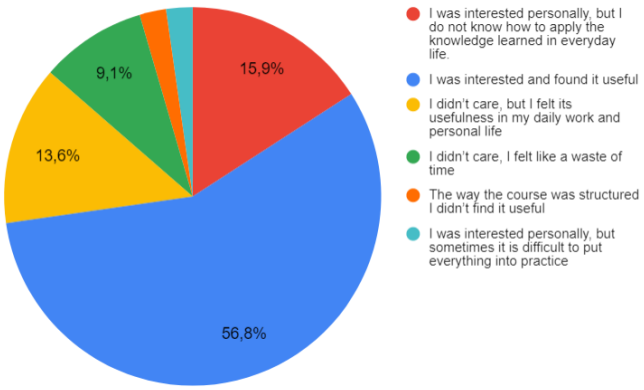

Figure 4.9. Usefulness perception for passive training

Considering **the change of behaviour** achieved through training (a reference to optional open answers):

- 4 users declare that they have not changed their behaviour as a result of the training received. Some users believe that they have modified their habits only in part with an increased sense of anxiety about the danger, but without a real perception of benefit. For someone, increasing risk awareness increases the sense of inability to recognize the world of cybersecurity/insecurity too vast.

  > "I have changed my behaviour only partially because I am aware of the risk, but I would need to be able to use it daily, whenever I turn on the computer for both work and for my free time until now, I feel inert in front of this vast world!"

- Other answers indicate greater attention to the entry of their data on the network, online purchases, passwords, cookies, sender e-mail addresses, privacy protection, attention to information found on the network.

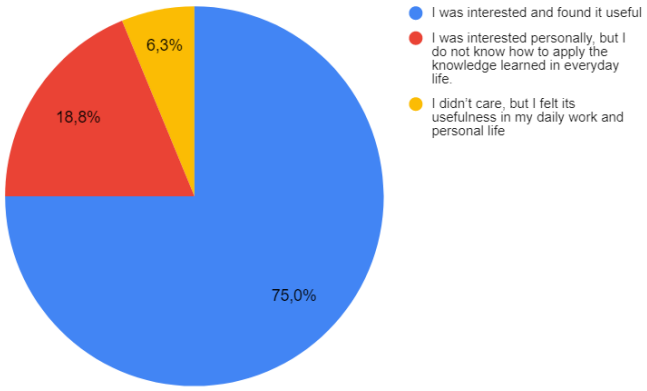

Figure 4.10. Usefulness perception for active training

Considering separately users who have had active and passive training:

- 11 actively trained users shared their experience in terms of behaviour change. Of these only 2 claims not to have changed their habits. The others declare greater attention, awareness of the reasons why it is important to protect themselves.
- 28 passive trained users shared their experience. Of these 18, they claim to be more concentrated when they enter their data on the network, password management, attention to information shared and read on the network. However, 10 users do not consider their behaviour modified.

Considering the change of behaviour, active training appears to be the best teaching technique. In relation to the answer obtained the user behaviour with active training changes about three times more in comparison with passive training.

4.1.5 Game elements

Almost 94% of the total participants are in favour of the introduction of gamification in the workplace in relation to computer security training. Only 13 participants were unfavourable.

Comparing the two graphs 4.11, 4.12 is shown that socialization and cooperation are among the most chosen elements (66%) and, on the other hand, the competition between colleagues is the most discarded element (74%).

Secondly, for the chosen elements there is physical interaction with tools, immediate feedback, competition between teams. In addition, two new elements are proposed: theatrical improvisations and levels to overcome.

As for the discarded elements, after the competition between colleagues, there is the competition between teams and the reward/recognition.

These choices are motivated (free open questions) by recognizing the **competition between colleagues** too stressful in an already often competitive environment. Competition between colleagues, according to most participants, could cause internal problems and shift the focus from security. In addition, it is not recognized as useful during the learning phase.

> Competition between colleagues is useful for the game, but it may not be in a working context for relationships between colleagues.

> I would reject the competition because it is already too present within the teams and I think it is not a good method of learning.

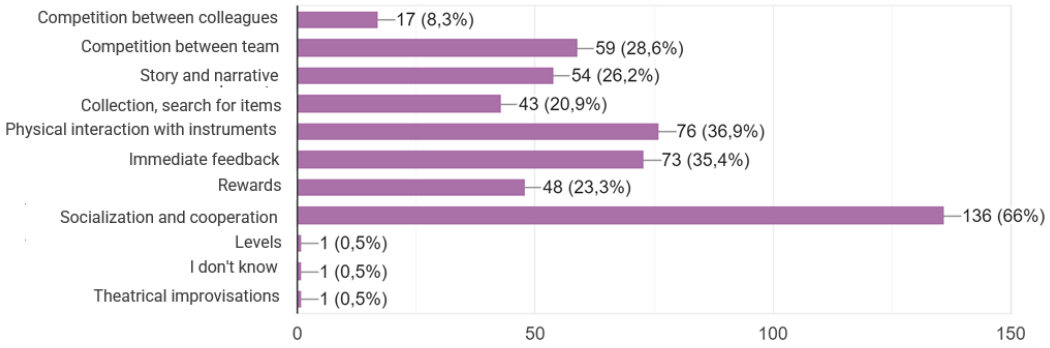

Figure 4.11. Game elements preferred

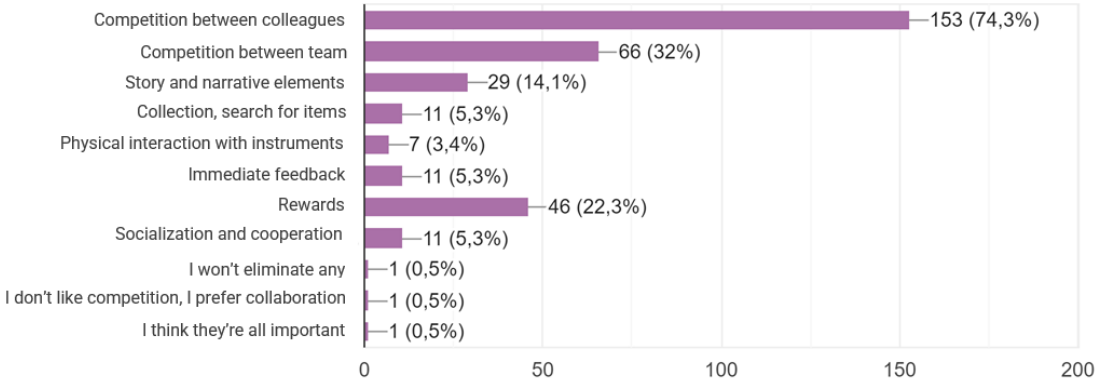

Figure 4.12. Game elements excluded

The **rewards** are rejected for two main reasons:

- Competition:

  > [...] Having prizes or rewards would lead to competition between colleagues.

- Inadequacy compared to the working environment:

  > I find rewards in some way inadequate, thinking that you give the dog biscuit if it raises its paw.

On the other hand, **collaboration and competition between teams** is recognized as a moment of socialization that can lead to an improvement of the internal harmony of the group.

> Teaming is the winning element of every company. Every action must be aimed at strengthening and not weakening the group.

Another positively motivating element is **physical interaction with tools**, recognized as crucial especially for the computer science environment.

> I selected physical interaction because I think that simulations are the best way to understand computer topics [...]

However, the **narrative elements** have obtained conflicting motivations:

- For someone it was considered boring, distracting from the final goal.
- For others, storytelling makes it easier to understand concepts.

Comparing **the selected/discarded game elements by age range**, it is possible appreciate the results reported by the graphs below 4.13, 4.14.

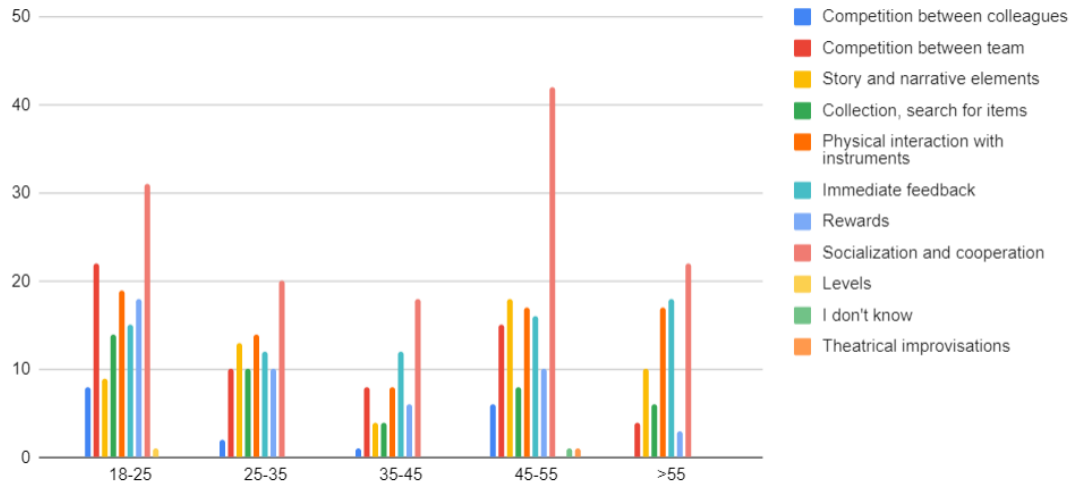

Figure 4.13. Game elements preferred for age range

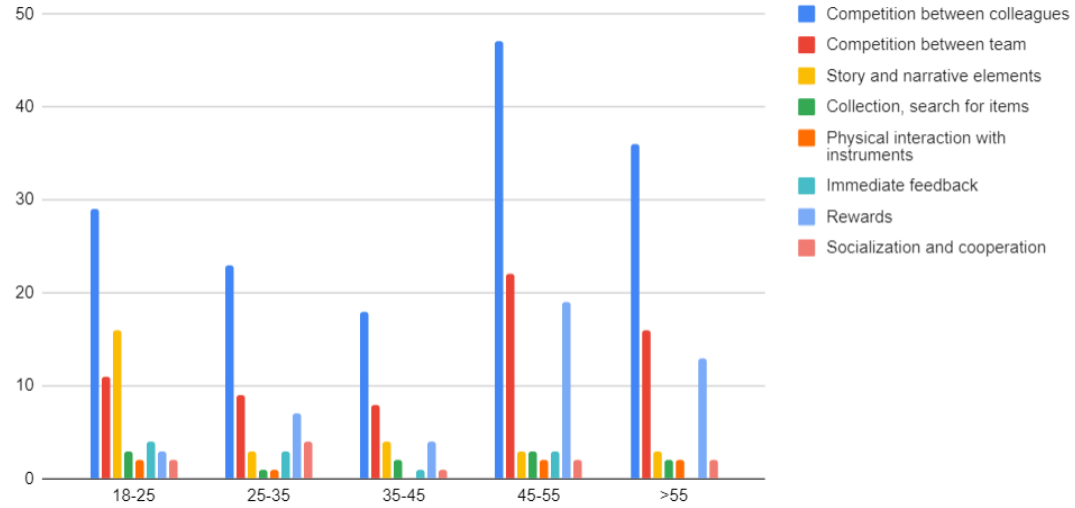

Figure 4.14. Game elements excluded for age range

It can be noted that in all age groups the most chosen element is socialization and cooperation. Although with distinct levels of preference, the preferred elements are comparable in all ranges. A separate note for the "rewards": they are preferred in younger groups and gradually discarded as the age groups grow. This element can also be noticed by the graph of the discarded elements.

For the discarded elements, for all age groups, in the first position, there is the competition between colleagues, followed by the competition between teams. According to the younger group, the elements of storytelling can be excluded, but this trend is not found in the following age groups.

Looking at the graph of discarded elements, physical interaction with tools, collection and

research, socialization and immediate feedback is the least excluded elements from participants (in some age range these elements have not been discarded even once).

Considering only the responses of **users not favourable to introduce game elements within the working environment** (13 participants): for the chosen elements 4.15 socialization and cooperation is always the preferred element with 25%, followed by the narrative elements 20% and immediate feedback 20%.

It is important to also consider the idea of the people not being interested in the introduction of the game in the work environment because reported [20] the probability of abandonment in users not voluntarily interested in participating is much higher resent by users favourable to the game. So, it is important in a cybersecurity field to find a correct compromise with all the possible users.

Also, with regard to discarded elements 4.16, the competition between colleagues is the most excluded element (50%) followed by the competition between teams (17%).

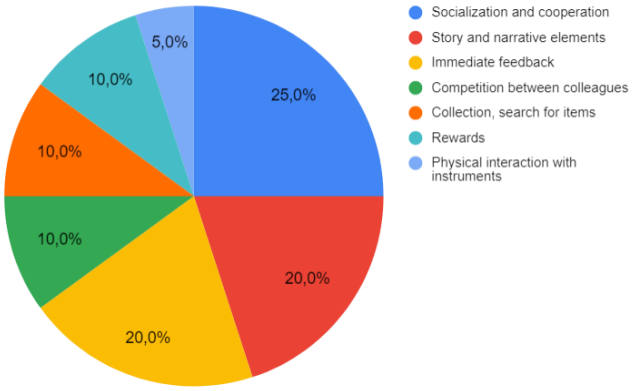

Figure 4.15. Game elements preferred for users opposed to introduce game elements in working environment

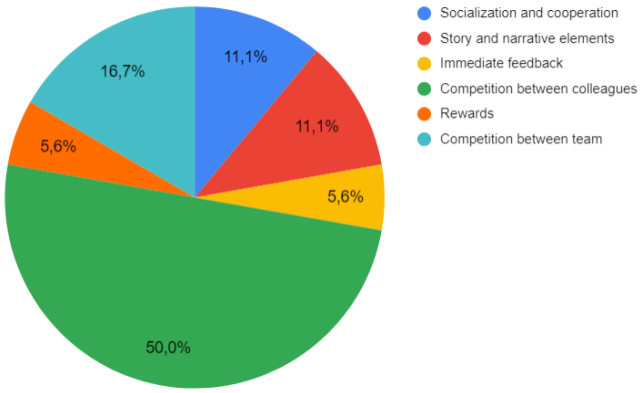

Figure 4.16. Game elements excluded for users opposed to introduce game elements in working environment

It is possible to notice that users without interest in gamification prefer socialization and cooperation and immediate feedback as the other users. But one of the less preferred elements is physical interaction with instruments, this element is one of the most differences between all the users. On the other hand, story and narrative elements are well accepted.

To know **real cases of attacks and vulnerabilities** near the user environment would be appreciated for 90% of respondents, 9% no, while a person has expressed their fear of knowing

risks close to it. So, trying to intrude real incidents or anecdotes into the education process should be a great starting point to involve more people as possible.

4.1.6 Final comment

Thanks to other comments left by the participants, it is possible to notice some elements:

- They express the difficulty to protect themselves if far from the study or work environment:

  > It is difficult to feel invulnerable and really protected from attacks. It is a huge world and unknown to most, even for this reason it scares.

- Other recognize as fundamental an education since the first years of primary school:

  > In order to drive a car, you need a driving license. To use a PC or a smartphone nothing is required.

- Other express their difficulties and doubt in managing security related to many passwords to remember and how to know if their data are vulnerable.

4.2 Gamification experts

In this section are summarized the information obtained thanks to the dialogue with gamification expert: Professor Francesco Lutrario and the Project Fun community.

The aim is to analyse the main differences and application features of gamification in cybersecurity. Inside the gamification application, the most subcategory used related to cybersecurity are Serious game, Capture the flag competition. However, it is also possible to find experiences more general without a specific name, described under the general category of gamification. The section also considers the suggestion given by experts.

4.2.1 Gamification categories

Serious game

Serious games are real and complete games used with the purpose to teach something and not only to have fun. In cyber security, it is quite common to use of serious games especially when the participants are potentially many and not experts.

This site shows the most important serious game about cyber security [105]. The environment most used are the school (mainly university) [106] and work [107]. The purpose of the games can be different: take the best decisions in a limited time [108], avoid future attacks based on daily actions, training against major network vulnerabilities such as phishing, malicious websites, compromised devices and social engineering [109] [110] [111].

The serious game, being a game created completely, although on a serious topic and with the aim of creating new knowledge allows its reuse at different times with different user groups. A serious game already implemented can be reused with different students/users/colleagues. It also allows maintenance that is easier to manage: the updating of the system can be done directly on the product (server) compared to a precise reorganization related to the single fruition environment.

However, a limit of the serious game is not to be able to take into account users in the specific if not by dedicated range (specific working environment or precise age group). Modifying the game with respect to users at the moment (based on their characteristics and specific skills) is very difficult if not impossible.

Summing up, serious games are often used in cyber security to interface with a category of users (such as workers or students) and consider a standard level of knowledge not modelled on

the individual student or situation. This definitely helps to standardize the product. The main limitation is that rarely the game is created ad hoc on the end-user with its precise characteristics (not only with respect to the categories of which it is part but also with respect to its individual skills/ characteristics) or on the group of participants examined.

Slightly different from the pure serious game there are the cyber escape rooms [112]. They can be both online and on-site. It is a team game in which gamers need to discover information to solve the proposed case. In some cases, different teams play by trying to figure out who and how stole sensitive data. The game is developed through a series of clues that had to be analysed by searching the desk, PC or suspect email. In this case, is possible to build the game on the people features and the security problem linked with the specific environment. So, it is possible to adapt the escape room both to the environment and to new attacks or vulnerabilities that emerged, that can always update the employees to the new dangers. But it is also clear that each game needs to be structured and reorganized each time, especially if it is done in presence.

CTF

The capture the flag competitions are playful experiences, usually concentrated in a few hours (24-48) in order to put into practice technique knowledge closely related to the cyber security world. Usually are organized in teams with the purpose to find the hidden flags using hacking techniques [113].

There exist some different kind of CTFs [114] [115]:

- Jeopardy: usually online, there are presented some challenges to solve them is necessary to find the flag, each flag gives to the team some points. At the end of the game, the team with the highest number of points wins. Usually, inside the team, cooperation is needed to divide the challenges and solve as many problems as possible in a limited time.
- Attack/ Defence: each player or team have a virtual machine. In this case, each team have to defence its services and attack the other teams. The points are assigned on the base of flag stolen in a limited time, there are also point for the defence phase.
- Boot2Root: usually for individual users, the gamer has to exploit vulnerability inside a virtual machine with the purpose to obtain the root privileges.

As shown in the chapter before, CTF should be organized in different environments, but it is necessary a deep interest in the subject, the level of initial knowledge can also be minimal but it is important that the user has an innate interest in computer topics often in a technical way and not just daily use. CTF competitions allow the user to understand how algorithms, encryption, reverse engineering, web application vulnerability work by acting and thinking like an attacker. CTFs allows the gamers to apply theoretical knowledge, usually learned during the lessons, in a practical and fun way in a protected environment, allowing a deep understanding of security issues, techniques and technologies.

The most common environments in which it can be found are school or work related to environments strongly connected to computer security. It is also possible that CTFs are organised by separate companies and participation may also be extended to external users or students (for example [116]). In some cases, some preliminary training is provided in order to prepare the users for the competition, in other cases the users need to already be prepared and they do not receive any hint or learning phase. The principal aim is to increase knowledge in network topology, protocols, best-practice, communication protocols like IP, TCP, UDP, NAT, secure channel and standard solution like TLS and software update, principal type of attacks like DoS and Man in the middle [117].

Increasingly frequently CTF are used to form the future security experts [118]. This aspect denotes a technical characteristic of this gamified competition of this gamified competition and a growing need for cybersecurity experts.

In classic CTF is possible to find as game mechanics physical interaction with tools and technology, competition between teams, socialization and cooperation within the team, reward

assigned on the base of points and leader board. Another essential element is that almost always the participation is voluntary.

On the other, end there exist some platforms that try to use CTF schema to form their users. For example, ImmersiveLabs is a platform used to empower organizations to increase, measure and demonstrate human capabilities on cybersecurity [119]. It is used for more technical aspects like technical tools, reverse engineering and malware. It aims is to continuously update and challenge users in order to be ready for crisis simulations. One of the important aspects is that it uses gamification. The main mechanics used are:

- Interaction, exploitation and incident simulation. The idea is to make the scenario as real as possible in order to involve the users in the learning phase and not only to complete the task.
- Story and narration, each simulation is set in a specific area and environment. In this way, users have to think as the environment proposed like a criminal organization, or healthcare provider and airport terminal. In this way, users have to create a mindset different for each situation.
- Challenge, the users have to solve tasks like a CTF exercise in order to challenge themself and the teams.

To date, the main limit about topics covered by CTF is that usually, they are focused on the technical aspect leaving aside other important aspects like safety management and regulations. As mentioned by [120], social aspects, privacy, cyber low are not covered by CTF challenges. The study report that comparing the topics presented by Cybersecurity Curricular Guidelines [121] the cryptography and the network sector are the most presents topics. On the other hand, cybersecurity awareness and regulations are the last present. It is possible that in the future CTFs will also integrate regulations and consider human aspects.

Gamification

Gamification, in general, does not have precise rules or fundamental features recognizable (as is possible to notice in CTFs and serious games), being free from prefixed schemas can be applied in any field with any type of users. The main advantage is that it can adapt to the situation and level of knowledge of user (children, teenagers, adults with or without experience in security).

The main applications in the field of safety can be found in a school environment with a limited number of users and referred to a specific target or built for a wide but well-structured audience on specific user's skills. Therefore, the study of the target can be carried out in two main ways:

- Known users: it is well known their level of knowledge, interest in the subject for example based on their precise study path.
- Target chosen a priori, desired level of final knowledge without keeping into account the previous knowledge of the users. This is used, for example, in the training phase during the onboard company process, because it is necessary that the user know some specific concept. In this case are considered age range, profession and environment of the application.

Before defining the mechanics and dynamics to be introduced into the experience, it is good to understand which target we are referring to, in which environment. Gamification in general, being freer, can adopt both analogue and digital platforms (as opposed to CTF and SG where digital interaction is preferred). It is possible to change the standard lessons in a more inclusive way open to new experimentations. The research [20] highlights the synergy created both by the lectures and by the use of an online platform.

Gamification, if on the one hand there is a strong personification and adaptation of the activities built on the target, on the other there is also a large phase of analysis and initial research. This element is not negligible also in reference to the time needed to contract gamification on cybersecurity topics.

4.2.2 Suggested elements

Thanks to the interview with Professor Lutrario Francesco, an expert in gamification, is possible to define some elements to keep in consideration when a gamified process is designed.

He suggests discouraging the use of points, badges, leader-board if not well thought strategically. It is important that the user feel as in a real free context in which he can experiment without the fear of making mistakes. Especially in the working environment, gamification works only if the user feels free and is not afraid of repercussions or punishments. If the users perceived some possible metrics or elements that should be used against them the game fails its work and also the learning phase is affected, because the cognitive process is not activated in the correct way.

Often gamification is extremely simplified only adding points or leader-board in a standard environment. Professor Lutrario call this process "Pointification" and express his disappointment about the process created only by adding points or badges inside a project without thinking about the real mood created in the user inside the specific environment of interest. Leader-board and comparing colleges each other should be a source of anxiety and stress [122]. This aspect needs to be stressed in the cyber security environment, in which the user needs to be well disposed to change his habits and learn new elements for his and company safe.

For these reasons, to use "Pointification" should be a huge problem because can lead users to a competition based on their own ego and not focused on collectively. Instead, it is recommended to create a motivating and inclusive environment.

This reflection opens the door to another problem related to networked platforms that are defined as gamified. Definitely add directly points to a process to create a game-like environment is easier [123] and should be managed automatically by a server or by a computer program. Also comparing the huge quantity of LMS present, they offer a default integration in the learning process of gamified elements. But the problem is that usually trivialise the gamified process offering only points, badges, tests and monitoring actions. The use of this platform forgot the creative idea of the game. It is important to remember that the game also include creativity, sharing and experimentation.

In order to categorize the platform used for the training nowadays, it is possible to distinguish in three categories [124]:

- LMS: Learning Management System, used to monitor and deliver training courses. It is more active for the user that can interact with the platform in order to learn something.
- CMS: Content Management System, organization of multimedia content without meeting training needs. It is passive for the users, like a blog or a website.
- LCMS: Learning Content Management System, includes both functions.

In many of these platforms the gamification is integrated with the system. Some of the most used solutions are:

- Open edX: it used as mechanics points liked with actions called "events". The most effective types of events are viewing videos, getting a certification, writing notes, solving problems. Other mechanics used are badges, collected after a certain amount of points earned. it is possible also used a leader board based both on the points and badges obtained. For the instructor is possible to manage points and badges and choose combinations of events in order to obtain a new badge [125].
- Moodle: inside this platform is possible to add some plug-ins to include gamification inside the course organized. It is possible to add levels and progress bar, ranking, points, coins and badges, quiz [126].
- Kahoot!: it is used to create quizzes and slides with user interaction. It is possible to earn points and badges on the basis of the result obtained [127].

- PlayOff: more concentrated for companies it is used with the purpose to monitor and motivate the employees in the HR process. The main mechanics used are metrics like points and action used to track the users and set rulers and conditions. It is also possible to use a leader board on the basis of the metrics used. Another important feature is that it is possible to create teams as subsets of players [128].
- Viewhooo: it is a platform to create interactive slides with the purpose to combine presentations and gamification. It is possible to use it both for education and business purpose [129].
- Mambo: is a gamified platform to engage teams and measure activities. Compared to the other platform it gives tangible benefits as coupon system as rewards system on the basis of points earned during the experience. These coupons can be exchanged for discounts or shopping [130].
- Talentlms: in this LMS it is possible to include in a customized way some gamification elements. For example, points, badges, leader-board, avatar and rewards. [131]
- Skillato: is defined as engagement and continuous e-learning for business performance. The principal aim is to motivate and reward people that achieve their goals, but at the same time motivate and encourage users that do not achieve the objective. In this case, it uses the micro-learning structure, incentivise the use of the platform little time per day but constantly. [132]
- Gametize: it is a platform to create an involvement project. The principal mechanic used is the challenge, it is possible to choose from distinct types of challenges based on quizzes, flashcards, secret codes and QR codes. The users win points after overcoming a challenge. Another crucial element is that users can collaborate each other to solve the problems proposed [133] [134].

As is possible to notice, many of the analysed platforms propose as main mechanics points, badges and leader-board. It is obvious that these mechanics are comfortably manageable with a computer system, but often they are not enough to create an effective gamified system, as explained by Professor Lutrario. It is also obvious that the use of these platforms helps the instructor to organize the work without starting development from zero, but with an initial e common structure. The ease of use can however affect the final yield if not well adapted to the context with the correct and useful elements of gamification for the target. Therefore, it is clear that also chose a gamified platform need a correct analysis in the initial phase.

Another point expressed by Professor is that every process is different with another, each company can have its own dynamics and precise internal rules. For these reasons, following or creating a fixed schema is useless and risks bringing more problems than benefits. At the same time, using a predefined LMS or gamified platform should be a problem with the integration of personalized elements.

4.3 Cyber Security Expert

Thanks to the experience of Professor Yanick Fratantonio, an expert in cyber security and creator of MOBISEC EURECOM challenge wargame, it was possible to collect interesting information directly in cybersecurity education.

The MOBISEC course is a challenge wargame used inside a university course with the aim to incorporate standard lectures with practical implementation. According to him, the use of the challenges and practical implementation gives to students the possibility to deepen topics learned in class. This structure should benefit students that already understand the theoretical lecture, thanks to the possibility to apply the content in a real context. At the same time, also students with more difficulty during the standard lecture can have benefits: often apply in practice what was taught is easier than student thought.

The correct balance between practical and theoretical parts is complementary for both of them and one can help the understanding process of the second and vice versa. The possibility of challenge contributes also to the definition of soft skills and to the increase of self-confidence necessary in a future work environment.

The work created by Professor is available for free and it is focused on mobile security on Android, for the challenge section is structured into three homework:

- Android App Development and API
- Reverse Engineering
- Exploitations

Each homework is structured in 5-8 challenges, students can upload their solution and obtain points if they capture the related flag. At the end of the semester, the points obtained from the challenged system is valued for 40% of the total grade.

4.3.1 Gamification Elements Used

The game elements used are:

- Public scoreboard, the students are invited to create a nickname in substitution to the real name, only the Professor know the real link between name and nickname. However, was noticed different approaches from the students: some of them prefer to use their real name and other nicknames, there is not a correlation between this choice and the actual student skills and outcome obtained. The possibility to create anonymization was created both for positive competition and for creating an ethical hacker mood and so immersion. The scoreboard is not considered for the final grade.
- Helps and Hint, Professor was available to help students and answered all questions in a private way. In this way, Professor follows the role of guidance and avoid unnecessary waste of time. The instructor has also the responsibility to create a welcoming environment and encourage dialogue also during the theoretical lecture.

4.3.2 Suggested Elements

He suggested us some elements to create a useful gamified environment for cybersecurity:

- Avoid stress factor, in an education environment users are free to participate, there is not winners or loser.
- Avoid guess elements: only guess should be very frustrating. It is important to create a logical schema in order to find the related flag.
- Avoid big code and prefer little bugs in little lines of code. In an educational phase, it is not necessary to be realistic, because in the gamified experience the focus is to understand the problem in order to be able to identify it in future and harder environment.
- Avoid losing time, having some hints or guide is useful in order to do not lose the focus on the problems and lose motivation.
- Challenges have to be focused on precise skills and not a specific real case of specific tool.
- Train one skill at the time, as basic blocks, only in the final levels is possible to put more than one skill together, but only after consolidating one at a time.
- Create a public blog or newsletter in which gives common hints, information or suggestion useful for everyone. For example, how to debug in a local environment, how to use logs to understand the test settings and where to look for general programming information.

One problem encountered was the availability of the student to interact with the Professor asking for doubts and problems.

4.4 TLLab and Teaching week

The Teaching and Language Lab is a project inside Politecnico di Torino created in order to create moments of comparison between the professors at the university and the experimentation of new teaching techniques. They organize the "Teaching week" ("Settimana della didattica") between 14-18 of February 2022, during the week were organized several seminars with experts in the education environment and with Politecnico Professors' that reports their experiences in the application of active learning methods [135].

4.4.1 Experiences

The focus of the seminars taken during the teaching week was how to allow inclusion and active participation, critical thought and creativity in large classes also for STEM subjects. They present different strategies, contexts and with different students target:

- During the first-year students are less motivated in technical subjects such as Maths. In order to stimulate reflection, questions, use of own notes taken during lectures and reorganization of thought in the same moment of the presentation of the new arguments Professor Morando use as instrument comparison between peers. The lecture was structured as follows:

  1. New content explanation in standard way
  2. Group work in class
  3. Submission of each group solution and visualization of the class results (self-evaluation)
  4. Discussion with all the class about more critical elements and errors
  5. Students' questions

  The group assignment present must ask for final delivery, encourage comparison with the other students and use the notes just taken. It is also possible to create individual assignments after the lecture with a similar structure in order to train students.

- In the context of a more technical lesson, Professor Giaccone explained the use of tools as notebook in order to teach abstract knowledge, avoiding the student attitude to postpone the consideration of the topic at a later time. In this way, the lesson is organized in a contrary way to the standard lesson: first of all, the results are presented visually and only after the abstract formulas are explained.

- Professor Zotteri explain his experience with the Harvard business school techniques, based on analysis of case studies, to create a discussion in the class and introduce new elements and theoretical solutions. The work is organized as follow:

  – Before the lecture, students have to study autonomously a case of studied assigned and answer in little group questions proposed by the professor.
  – In class, the professor guides the discussion between students on the case proposed in order to activate reasoning and internal comparison.
  – In conclusion, the professor guides the discussion at the pre-organized lecture aims.

- In the context of the OCSE project, which tries to understand if creativity and critical thought are training skills, some courses of Politecnico di Torino were involved. In particular professor Graziano shares her experience. She organizes different moments inside the lecture in order to activate students both with creative experience and during the theoretical lecture. During the lecture, she organizes some "active time" to create active learning regularly to make students aware of developing critical thinking.

  Some experience organized are:

  – The creation of mental maps on the content presented during the lecture and shareable with the class.

  - Group work, using classes with physical organization and furniture to work on group, students are called to answer to question proposed by professor with their group and share their solution with other thanks to collaborative tools like padlet or similar tools. The questions proposed by the professor does not present unique correct solutions, it allows for different interpretations and resolutions.

4.4.2 Results and suggestions

The use of active learning, in general, all professors agree that should help in different contexts:

- Group solutions are more correct than individual answers, comparison with peer usually help the comprehension.
- Professors should monitor the class trend, progress and recognize the most difficult topics.
- Student involvement raises the level of attention.
- Improved long term memorization using associated memory and emotion.
- Presentation of complex reality closer to the work environment, not all data are available and there exists more than one way to find solutions.
- Students that are actively involved drastically reduce the time to dedicate to studying later, for example in preparation for the final exam.
- Training of soft skills likes to communicate, interact, negotiate, debate, decide, ask questions, useful in the work environment.
- It is possible to use new tools and technology to interact with the class, make polls and brainstorm in real-time.
- Use quiz is suggested for questions that induce students to reflect on complex problems or to compare elements. On the other hand, quizzes are discouraged for notional questions.
- Explain at the beginning of the lectures the goals of the day.
- Work on "error education", teach to the students that have doubts or make errors during the lectures is normal and accepted.
- The professor has the task of creating a relaxed atmosphere that encourages dialogue and participation of all. It is important to keep in consideration reaction in front of student errors, and different student personalities.
- When it is possible is suggested to use external testimonies like ex-students or external experts.

4.4.3 Issues encountered

Although the benefits outweigh the problems, active learning has presented difficulties and limitations in almost all professors:

- Not always students are glad or accustomed to participating, in this case, it is important to explain and convince them that they are doing something useful for them both in the context of the specific course and for learning soft skills.
- The error culture is not yet well accepted by the students, a lot of students are scared about interaction with the class.
- Professors have to restructure the lecture and schedule in a precise way all the practice activity considering the time limitation in relation to the course program

- Time managing is not an easy task both considering the student's efforts and professor organization. For the students is important to consider the time spent in relation to work in and out of class to avoid additional stress elements. It is clear that active learning is more time consuming than standard lectures if it is not well and precisely organized. One possible solution is to start to dedicate little time, for example, three minutes, for lessons and then increase as needed.
- Students and professors often have difficulty distinguishing between the education and evaluation level.
- Professors have to know how to use tools and technologies proposed.

Chapter 5

Methodology

This chapter summarizes the methodology elements needed to create a useful gamification cybersecurity experience thanks to the information gathered in the previous chapters. In particular, there are used information gathered thanks general information and framework about gamification presented in chapter 2, results of previous studies and frameworks directly focused on gamification or serious game in cybersecurity presented in chapter 3, users and experts suggestions presented in chapter 4.

5.1 Cybersecurity skills and topics

As the first element it is necessary to focus on cybersecurity skills and topics on the base project aim, target, user's previous knowledge, attitude and aims of the education program.

In order to organize the topics is possible to categorize each element in section and subsection in a logical way and following the guidance. It is also important to organize and identify the precise skills needed in relationships with the topics selected. For this purpose, it is important to choose and use an official database and information.

For **technique education**, the COFELET framework suggests to follow CAPEC and NCWF guidance in order to organize the syllabus and link the correct skills.

Using CAPEC it is possible to understand real attack patterns organized as a dictionary, CKC is the cyber kill chain and should be used to understand and analyse the structure of a cyber attack model and thinks to mitigate elements. On the other hand, the use of NCWF is concentrated on the definition of skill necessary in cybersecurity for category, areas and work roles. For each category is defined precise abilities, knowledge, skills, task and capabilities indicators needed for the user's role.

For **everyday users**, in addition to cybersecurity awareness topics, as explained in CybAR project it is important to include some elements in order to structure the content:

- **Perceived Susceptibility**, the personal probability that attacks influenza the user. Each thread presented in the experience has the purpose to influence the user's perception thanks to the immediate feedback received during the experience.
- **Perceived Severity**, user's perception of negative consequences. Each wrong action leads to countermeasures proportional to the error inside the game environment, in this way user can understand the seriousness of the threat.
- **Perceived Threat**, show the harmful consequences of the following attack so you can overturn it in reality.
- **Perceived Safeguard Effectiveness**, thanks to helping and suggestions users learn to recognize thread and act consequentially in a later stage.

- **Perceived Safeguard Cost**, perception and estimation of physical, cognitive, time, money, recovery effort and threat recognition.
- **Self-Efficacy**, create self-confidence and trust the safe action presented. The experience aim is to create knowledge for independent users.

It is also necessary to add to specific cybersecurity knowledge also precise topics, policies or elements related to the environment considered as personalized elements.

It is obvious that different purposes of usage involve different possible audiences, for this reason, to organize the work it is possible to use the Bloom theory in the cognitive domain. For example, for a not technical expert could be enough to concentrate on memorization and knowledge, on the other hand for the technical aspect it is important to analyse, vaulting and create.

5.2 Tools and technology used

It is important to choose the **type** of gamified project, for example, CTF, serious game, scavenger hunt, virtual or real environment, web-based application, board game. Consequentially, it is also important to choose the correct **technology and tools** needed to create the experience. It is also fundamental to choose the correct system that can support the project both in technique aspect, in scalability and the fruition accommodation. For example, in mobile security environment was chosen CTFd and android emulator and it was deployed in a local server.

For this purpose, it is relevantly considered the target and how they have to **interact** with the system, considering their previous knowledge and experience about the interaction desired way. During this step, it is necessary to highlight what the users have to do during the fruition. For example, in 6 students have to create a game, instead of in 5 users can interact with the web application to obtain information.

Another crucial element to choose and organize in this step is the effective material used during the experience collected as **teaching content** and material and its format (text, imagines, videos).

5.3 Rules

The game rules have to be explained clearly and minimally, easy to understand for all the users. In the rules, it is necessary to specify what is allowed and which countermeasures are taken in case of attempted fraud. For example, in MOBISEC project students failed the exam if find flags using the code of other students. In other cases, is possible an intermediate solution, for example, losing points, blocking the challenge for some minutes or in extreme disqualification from the game. It is important to remember that for users what is not declared as denied is allowed.

In this section is also possible to explain which kind of technology have to use and in which way, including also prerequired skills and abilities.

The rules need to be clear and they are also useful in the first level of the game as a guideline for the player in the onboarding phase. To respect the four freedom elements is necessary, but rules give guides and, in some way, route the resolution of the problem to avoid initial discouragement and a sense of loss that would cause immediately abandon from the experience. To give too much freedom in the experience should be counterproductive 6.

5.4 Gamified elements

5.4.1 Challenge

Inside the challenges, it is possible to find the content of learning and learning goals already set in skill and topics sections. It is possible to structure the challenge lifecycle as a real attack step:

1. Initial Compromise
2. Establishing Foothold
3. Privilege Escalation
4. Internal Reconnaissance
5. Lateral Movement
6. Maintaining Presence
7. Completing the Mission

It is also suggested to create the challenge **focused on security issues** and not on the use of a specific tool or programming language, the use of the tool is only the means to reach the solution. Moreover, it is not necessary, and in more cases discouraged, to recreate a situation as actually happened in reality but concentrate on the skill useful for the user in a real and future context. For example, it is possible to simplify a real case of an attack to present specific issues or competence needed, in this way it is possible to remove further difficulties, which although real, are not focused on cybersecurity elements and experience. During the Fratantonio interview, he suggests using short code with little bugs instead of many lines of code in which it is easier to lose the general meaning.

It is also important to create the correct balance between **guessing elements and randomization**. If the solution is too easy or, in the same way, too hard to be guessed it is possible to create issues with the flow theory. Challenge solutions need to be found with a logical structure not only based on guessing element and need to be feasible during the game time and users' patience.

In the education environment, more specifically in high school, it is possible and useful to include cybersecurity topics in other subject modules like Mathematics, English, History. In this way, it is possible to create an experience that includes different aspects of the students' life and the students becomes aware of cybersecurity from more than one point of view. This **multidisciplinary** aspect, in the education phase, is necessary to deeply understand and be aware.

Challenges should also keep in consideration the attacks probability, damage and cost related to the attacks, cost of countermeasure taken in different steps during the attack lifecycle and cost of repairing 6.

5.4.2 Levels

It is possible to structure the experience in levels of progressive difficulty. Each level should be created on a specific skill chosen in the previous step and work on a specific competence. Structure the work as a **basic block** is a winning solution. During the last level, it is possible to combine different skills, already acquired, together.

Avoid unnecessary difficulties is suggested. For example, for brute force attacks, it is preferable to design brute force attacks manageable in little time instead of real brute force attacks that are too time-consuming. This element is important to avoid stress and frustration but keep the focus on the cybersecurity elements. What is important is to understand the meaning and do not waste time.

It is possible to structure the levels following the **psychomotor Bloom model**, based on users' level and desired outcome. For example, in order to create an experience for everyday life cybersecurity awareness imitation and manipulation elements are enough. Instead, for experts training is important to obtain precision and naturalisation.

In the level structure, it is also possible to choose and manage **prerequire** knowledge and structure the experience as a workflow with precise conditions and limits. For example, it is possible to create some blocking levels to verify precise skills and knowledge acquisition.

5.4.3 Hints and Help

In order to avoid wasting time, demotivation and frustration it is necessary to create some strategy during which users can ask for help. These elements could be managed in different ways: interaction with experts or instructors as in MOBISEC, hints freely provided by the platform as for scavenger hunt, hints can be bought or obtained as a reward during the experience thanks resources or level already acquired.

The way of interaction between the user and the instructor could be different but it is better to choose a unique interaction channel like email, real-time chat, social media or other technology for ease of management.

Creating some FAQ sections should be useful to manage the more frequent issues encountered by users.

5.4.4 Competition

In a gamified environment, it is possible to create competition between users or teams, there exist different ways to create competition. For example, to creating a **ranking** inside the gamified experience is the commonest way to create competition. Compare users should be a great idea to increase positive interaction and the desire for personal improvement. The scoreboard should also be seen by the users as a personal evaluation, comparing themselves with other peers. Other competition game elements are experience points, badges, level obtained, status, role.

However, it is important to keep in consideration some elements when a scoreboard or comparison metrics between users are used:

- **Privacy**: choose the correct structure in order to respect privacy and GDPR. For example, it is possible to avoid real personal names but invite the users to use a nickname or use a random string to unequally identify users. The use of a nickname in a cybersecurity environment could also be used to create an ethical hacker mood in the competition.
- **"Pointification"**: as expressed by Professor Lutrario, is important avoid, to summarizing all the gamified experiences as a collection of points, badges and comparisons of numbers. This element is important to create a useful gamified experience focused on acquired knowledge and not on the unsafe comparison.
- **Correctly evaluating the environment of use**, in some situations, especially the work one, creating a public scoreboard should be counterproductive because it would increase stress in an already competitive environment, as found by the questionnaire. It is important to evaluate the mood desired during the experience and choose or avoid elements.

A reasoned choice could be the one used in the MOBISEC project: there is a scoreboard, but it is not taken into account for the final evaluation, it works only as a motivator in an education environment.

5.4.5 Storytelling

Create a narration to make more engaged in the experience, it is possible to create a storyline that reflects the reality of the actual knowledge during attack or defence activity. In the beginning, the information provided is very little, as the story goes on more details are provided, with the completion of the narration in the last level.

It is possible to use a realist or not storytelling method, but the story must represent only a small moment of connection in order not to remove focus from the cybersecurity theme and not to bore.

5.4.6 Avatar

In order to create a user identity inside the game, it is possible to use avatars. With this gamified element, the player can personalise himself both in a physical way and for the ability or role assigned. Each avatar should be personalized for skills and roles inside the game and reflect the user role in reality.

As for the scoreboard, it is important to keep attention to the use of pseudonymity and anonymity.

5.4.7 Solution and answers

Creating a clear and precise evaluation system are important to create a trusted environment. For this reason, short answers are preferred as char sequences or strings. Chose a priori characters, font and format accepted is important both in the evaluation phase but also in the implementation phase, in order to avoid incompatible format errors.

It is avoidable open and long answered because it would be difficult to guarantee and quantify an impersonal, correct and accurate assessment.

5.4.8 Cooperation

Cooperation and user interaction are preferable in a work environment to avoid extreme competition. On the other hand, cooperation and teamwork should be also used as team-building experiences to increase cohesion between colleges. As reported from the survey, users would prefer cooperation and do experience with peers. In the cybersecurity context helping each other and collaborating with people with distinct roles and skills can create added value.

In education, context cooperation is more difficult to manage because of the final evaluation. There are some examples of use cooperation during the serious game creation in little team 6. Another element for cooperation could be seen as peers feedback provided during the presentation session. Gives students and users the possibility to interact with each other should be a create cooperation method as sharing information, but obviously, it was difficult to evaluate each student if the topics or problems analysed are the same. In the resource proposed 6 cooperation as peer reviews works because each student is concentrated on different and independent projects.

5.5 Evaluating metrics

In order to evaluate users, experience and outcome obtained are possible different solutions. This element has to be taken into consideration also in order to design the system and the experience for choosing the correct way to save, protect, manage, send and delete data collected during the experience.

It is possible to distinguish in two different evaluations:

- **Users' evaluation**. Some possible techniques are findable inside the game: compare users scoreboard and points obtained, compare number or type of badges collected, register the level obtained from the user, number and type of challenges completed. Other viable solutions are the use of event logging that reflect the user-system interaction like hints requested, number of attempts made for each challenge before the victory. In conclusion, it is possible to use external metrics like a survey or final exam on learning topics.
- **Project evaluation**. In order to evaluate the project, it is possible to use participation metrics and internal observation during the fruition time that rise problem encountered from users, availability of system and usability. Other metrics should be provided with users' survey pre, post and during the experience about level appreciation and knowledge acquired.

5.6 Feedback

Creating comparison moments during the experience as **fix and real appointment** could help the fruition quality. It is possible to create a comparison with different sources like peers, teachers, and external security experts in order to obtain ideas from different points of view and knowledge 6. In this way, it is also possible to obtain feedback in a different format and with different frequencies: peers orally and informally, professors write formal comments on the work provided and expert general comments or further information on the subjects presented.

Pre-organize specific moments of comparison during the experience, as the open day 6, help the users to organize the work during all project time, avoiding last-minute completion. Other possible solutions are represented by precise deadlines for which completing a specific task is required.

Other feedback elements should be provided with **graphical elements**, for example, progress bars. In this way, users can visualize its outcome and individual progress during the experience.

5.7 Elements of influence

In order to create an immersive experience on multiple aspects, it is necessary to exploit some elements of influence during the experience that could be additional motivation factors. Some elements of influence used:

- **Personal elements**, organizing the experience on the precise target with their interest and attitude should be a good idea to positively influence the experience. For example, the survey retrieves that in general users would like to know security aspects directly like with their work environment. Adapting stories and anecdotes to the environment and users considered would make safety more tangible and closer to users.
- **Famous people**, the use of people or characters known to the most for positive aspects could influence users to take part in the experience. An example is done by Paolo Nespoli in the Space Shelter project 1. Users' fans of Paolo Nespoli or interested in its themes will be encouraged to participate even if the main topic presented is related to security and not directly on space.
- **Persuasion**, it is the attempt to change habits and/or behaviour without the use of force. It is possible with two different strategies: influence people thought about an event in a rationally way or making an automatic process without changing thinking. Use of persuasion usually includes humour, competence, repetition, intensity and scientific evidence. It has been proven that intimidation and fear are counterproductive.
- **Social Proof**, this technique exploits people behaviour influenced by other users' experiences and comments. Public comment and evaluation of previous users should influence the new target to start the experience. The social proof should be used as the onboarding phase to start the experience, but also in the last phase of the user journey to compare users' outcomes with average results of other users and encourage permeance in the experience [69].

5.8 Elements to Avoid

It is possible to summarize elements to avoid in a gamified cybersecurity experience already expressed in other sections.

- In extreme competition, both the survey and the experts' experience discourage the creation of an extremely intense competition system.
- "Pointification" and use of fixed schema in different environments.

- Stress elements, users are free to participate or not, there are no rewards and a winner or loser. Related to the stress it is also important to consider the user efforts asked for during the experience.
- Avoid persuasion with negative emotions like stress, anxiety and fear. Especially because the issue is security users must be able to feel free, welcomed and safe.
- Rewards are often not coherent with the environment. It is strongly advised against economic earnings in the working environment. The idea of "if you do... you obtain..." do not work, because it exploits extrinsic motivator [136].
- Avoid communication errors: it is important to create the correct atmosphere between users and instructors with a trusted relationship [137].

5.9 Purposes of usage

The use of gamification in cybersecurity environment should be used for different aims:

- Training new technicians to cope with the lack of future experts in the field, reducing the learning time.
- Raising awareness in daily use more engagingly and effectively.
- Bringing new categories closer to the subject as women and young students.
- Children and parents' security online.

5.10 Fruition time and Update

Different sources suggest creating a long term experience during which create short sessions with a fixed appointment. During each session is suggested to present only one new topic and repeat it in different sections, with different levels of deeper.

It is strongly discouraged to create a unique long session once a year.

Other important topics are **continues learning** and training. **Updates teaching resources**, topics and events and adapt the work to the target that during the experience could change behaviours and attitude. For this purpose, it is possible to use eADR framework that uses implementation loops in order to periodically revisit and update materials. The framework is created by four steps: diagnosis, design, implementation and evaluation. For our purposes, the evaluation steps are important during the update. The framework also proposed an evaluation schema used during the evaluation phase. They suggest retrieving information about the user's reaction, learning, use of new skills and the learning outcomes.

5.11 Statical Schema

As support for the practical implementation, it is possible to use elements.

In order to correctly map and choose the learning and game element, it is possible to use the framework presented by LM-GM. There is not a fixed way to choose game elements and link them to the cybersecurity topics, and it is not necessary that all the elements previously presented are used at the same time.

The framework proposed two structures:

- Statical schema, in the statical schema is chosen the game element linked to the learning content and teaching material, with specification related to implementation and usage.

- Dynamical schema, dynamic representation of the workflow of the experience based on the relation forward choose between game and learning content. This schema is possible to use for difficult and more structured projects to be able to view the pattern of dynamics in action and in sequence.

Using both elements it is possible to schematize the game element, learning element, their implementation and usage. It is also possible, in the dynamical schema consider prerequire and conditions structure. The Dynamical schema is necessary for the design of serious games during which more games elements are used in a precise sequence, instead of in a gamified environment is also possible to use only the statical schema.

The LM-GM method already includes the Bloom theory to guide the selection of game elements in reference to cognitive levels.

5.12 Organization cost

In order to organize a gamified project could be useful to involve different experts: gamification experts, cybersecurity experts, technicians for physical and graphical implementation. The involvement of different experts may introduce an additional cost to the programme.

The strength of gamification can also become its weakness: adapting strategies and solutions in different contexts and projects are often not effective. Gamification needs strong personalization and is far from the "one-size fits all" strategy. It is a strong point considering that each project should adapt perfectly to the topics taught and the target audience, on the other hand, could cause additional cost in terms of time in order to design and create a useful experience suitable for the related environment [138].

Related to the time it is also important, and not an easy task, manage the time available to organize a gamified experience, for example in an education environment during which the time is limited.

5.13 Practical Use Schema

With the aim to create manageable guidance of implementation, here are briefly summarized the main steps to follow to create a gamified experience using the methodology.

1. Skills and Topics:
   - Select the target of reference (Technical/Non-Technical).
   - Organize in a logical way topics using standard guidance.
   - Select the precise skills needed.
   - Use the Bloom cognitive model concerning the target.
2. Tools and technologies:
   - Choose the gamified project type to realize.
   - Select the technology needed.
   - Organize the teaching content via tools and technology choose.
3. Rules definition:
   - Specify what is allowed.
   - Specify what is denied (if something is not specifically highlighted as forbidden it is perceived as accepted).
   - Specify countermeasure.

- If needed, prepare guidance for the technology used.
- Specify prerequired users' skills and abilities.

4. Game elements:
   - Select the game elements needed in the experience referring to target, environment of application, desired atmosphere, motivators, desired outcomes.
   - Use the LM-GM schema to organize and link each game element with a learning element and activities.
5. Organize evaluations:
   - User evaluation.
   - Project evaluation.
6. Feedback:
   - Organize fixed appointment with peers, experts, professors.
   - Use graphical elements like progress bars.
7. Element of influence: check if some elements of influence are needed in the experience to increase motivation.
8. Ensure that the elements not recommended by the methodology are avoided or at least kept to the minimum.
9. Fruition time and Updates:
   - Organize precise moments to checks and update both the system and the teaching content, keeping into consideration the target evolution.
   - Organize the gamified sessions in terms of fruition time.
10. Cost analysis: analyse the cost of the project considering experts, tools and time needed.

5.14 Role-Playing game

This section analysed ideas for future implementation using the methodology and tried to answer possible issues in a real context. As a game element, we focused on cooperation because it is the element less used in cybersecurity gamification applications but at the same time the most preferred by users in the cybersecurity contexts. Should be interesting to demonstrate the usefulness of collaboration and comparison. In pre-analysed experiences, cooperation is usually not allowed in order to avoid the sharing of results and procedures to discover solutions, for example in the context of wargames and CTF, and to facilitate evaluation in case of application at the education level.

5.14.1 Context and target

The target considered is students in Master of Science degree in computer engineering in cybersecurity, therefore the experience is designed for technical knowledge and new future experts in cyber security. With this consideration, the target is represented by a computer science background with a deep interest in cybersecurity topics. Participation in the experience is voluntary and the result is not used in the evaluation during the final exams. Each student does not receive a grade or bonus point for the final evaluation. The experience has as its exclusive objective a deeper understanding of cybersecurity topics allowing students the opportunity to train thinking critically by exploiting the knowledge and technologies presented during the standard lectures.

5.14.2 Cybersecurity skills and topics

As topics are possible to consider the solution, technology or protocol presented during the real course followed in the university path. However, the idea is that the experience should be at a higher level about the course fruition. At the same time, in the context of each course, each professor is free to organize the content and use the didactical elements that prefer. The topics presented during the courses are used as an available solution possible to choose after its run and blocked before. Each technology, once are available, are always possible to be selected. In this way, continuous learning is guaranteed.

For example, using as starting point the organization of the Master of Science degree in computer engineering at Politecnico di Torino it is possible to distinguish in four courses characterizing the Cybersecurity track:

- Information System Security (ISS), which are presented the main security issues in network computer systems, starting from the main types of attacks, authentication mechanisms, the base of encryptions, technologies like firewall, IDS/IPS, TLS, VPN [140].
- Cryptography (CRY), during which are presented the main cryptographic solution symmetric, asymmetric, hash function and protocol like DSA. In the same course, it is possible to experiment via programming with cryptographic primitives in C and python, by writing some little script to understand the main issues referred to cryptography [141].
- Cybersecurity (CYB), during which are presented advanced techniques to protect a modern network system. For example, PKI, secure network channel, wireless security, federated authentication, legislation, GDPR, forensic analysis [142].
- Security verification and testing (SVT), during which are presented as the main techniques and tools to perform verification and testing of an IT system. For example, are presented the main classification of security assessment techniques, vulnerability assessment, penetration testing, formal verification. In the same context, during the laboratory experience, it is possible to put in practice theoretical knowledge [143].

Each topic is divided into basic units available in the experience for students after its explanation during the lectures. The experience has as its aim train the students to critical thinking related to cybersecurity issues presented. In this way, students can define the best strategy to respond to a problem thanks to the information obtained during the courses.

5.14.3 Tools and technology

The tools and technologies used should be different for each run, considering the type of experience available and the topics analysed. For example:

- For the first experience, during which students are following ISS course it should be more theoretical and it is possible thinking to ask students for written reports, for example, shareable in some drive between all the team and supervisors to obtain feedback.
- When are possible to structure more practical implementation, think about writing code, for example during the CRY course, it is possible the use of virtual machine shareable. About it, one possible solution is represented by CrownLabs student project inside Politecnico di Torino [144].
- In the last semester, the CYB and SVT courses are run simultaneously. It is possible to think about the presentation of real or possible attacks/vulnerabilities. They could be proposed by real cases or by outside companies. Students, with all the tools at their disposal, implement possible solutions with code, theoretical solutions, CVE/CWE always based on the roles assigned to the various teams. It might be interesting, as a moment of comparison, to compare with actual solutions/strategies adopted in reality compared to those chosen by the students, both for attack and for defence.

As a common element, under construction during all the graduation paths, there is a sticker album on cybersecurity topics. Each time during a lesson a topic is explained for the first time, a card becomes available in the students' album. The album should be built virtually or physically. However, it is used as a facilitator and summary of known topics always available for students, and exploit motivator factor both for collections and progress.

5.14.4 Rules

The participants are divided into teams of two people, each team has a role: attack or defence. At the beginning of the experience, the context of analysis is presented for all teams. The context should represent a real, simplified situation or infrastructure in which some cyber security solutions are needed, and on the other hand, some possible vulnerabilities are exploitable.

Each team has a set of cards representing the technologies, solutions, techniques presented in class. These, depending on the reference period, will block or not, to respond to security problems can choose between the cards and combine them. The defence teams start to analyse the situation and choose, from the available cards, the best solutions to mitigate the security problems they have detected. At the same time, the attack teams detect vulnerabilities in the context presented and propose possible exploitation thanks to the know attacks patterns and consequences.

Professors or external security experts should give personal feedback to each team giving suggestions and comment on personal choices. In a public way, all solutions should be commented on in order to underline the best solutions and the main errors, anonymously. In this way comparison and a sort of evaluation is provided but avoid too intense competition between teams and prefers comparisons between topics rather than students.

Participation is voluntary and does not give any points for the final exam, in order to avoid pontification and extrinsic motivation. But its participation should help students in preparation for the final exams allowing them to think critically and study more concretely by applying the solutions presented, in a simplified context but close to the real one. This, in addition to the course, also wants to encourage the memorization of contents and their application in a future work context.

It is required the meet the deadline related to the submission of the reports or work proposed.

To avoid additional stress and a request for excessive effort for students, each student should dedicate the desired time to work on the project and the meeting may be organized at the beginning of the semester in order to make clear the commitments and make individual organization possible.

5.14.5 Gamification elements

The game elements proposed are:

- Challenge, focus on real but simplified problems and not tools. Elements of guessing and random are almost cancelled because it is based on elaboration and personal strategies (not a single correct solution).
- Levels, it is possible to distinguish in different organization levels:
  - During each semester it is possible to complicate the presented context in different episodes, with an increasing level of difficulty.
  - During all the Master of Science path, each semester and course add new elements and material all available for the students during the experience. In this case, it is important to keep in consideration for each experience pre-requirement.

  It is also possible to notice that during the first year each semester introduces new courses, but in the second year, the first semester is characterized by two cybersecurity courses. In this case, it is important to organize the experience thinking to new elements available from

all the courses that run in the same periods. It is also possible to use this organization to use the first runs basic block and the last one used to incorporate in a more structured way all the topics and subjects presented.

- Helps and Feedback, as elements of help it is possible to consider the standard lecture during which professors presented in a theoretical way the concepts. The professor should also represent the support figure in case of doubts. As feedback is organized a precise moment of comparison both in a private way and in public, with the aim to underline possible improvements and analyse choices.
- Cooperation, inside each team cooperation and comparison is needed to choose the elements in relation to the problems analysed. Inside the group is first of all important analyse the issues and replace to them in attacks or defence way depending on the role. The cooperation inside the team should be used as study and update moments. Each component of the team is responsible for the proposed solutions.
- Competition, between teams, it is possible to create positive competition, represented by the desire to choose the best solution in relation to other teams with the same role and respond adequately to the difficulties introduced by the teams from the opposite role. The competition creates avoid comparison between people but encourage the comparison between cybersecurity topics. For this reason, it is preferable to leave the reports and works proposed by teams anonymous, only professors should link each work with the related creator.
- Storytelling, in order to present the context of analysis and the various difficulties, can use storytelling to introduce in a more engagingly the situation and the role of the various groups.
- Motivators:
  - Progress, to create a sense of progress during all the experience paths, it is possible, in a graphical way, to present all the topics that will be presented in form of cards. Each set of cards will be available or blocked in relation to the standard program followed during the lectures. The possibility to see all topics starting from the beginning and see it's unlocked during the experience should create in students sense of progress as used by progress bar or other graphical elements.
  - Facilitators, the available cards are also used as facilitators for students because they have to choose from a limited set already known.
  - Condition, the available cards represent the pre-requirement to participate at the experience.

5.14.6 Evaluation

As mentioned before, the experience does not give points for the final exams or graduation, but after the first runs of the experience should be interesting to compare results of final exams with participation and not in the gamified experience. The idea is to understand how the experience should help students in memorization and understanding in a deeper way cybersecurity concepts with fewer efforts. For this reason, a reflection of examination trends is desirable, and the results of the exam should be a great comparison element.

On the other hand, in order to evaluate the organization of the experience should be created an anonymous survey to analyse criticism of the experience both from students and experts. In this way should be possible to change and modify the experience in relation to the motivator and ideas of the real users.

5.14.7 Fruition Time and Organization

In general, it is possible to think of three different scenarios, one for each semester of the first year and one for the first semester of the second year. Each experience is free and independent

from others for students of the cybersecurity courses. The only limitation to the experience is the passed previous exams referred to the course path. In the table are summarized the period, the participation constraints and the courses provided 5.1.

Period	*Participation constraints*	*courses provided*
The first year, the first semester	Enrolled in cybersecurity master	ISS
The first year, the second semester	Passed ISS	CRY
The second year, the first semester	Passed CRY	CYB, SVT

Table 5.1. Experience organization and constraint

Each experience should be provided with a pre-arranged schedule of commitments to inform students about the effort required and to create fixed appointments. In this way, it makes possible an organization distributed over time avoiding concentrating it in a few moments. The schedule must define the deadline to join the project, the presentations sessions, the deadline for the submission of works, the feedback sessions and the level upgrade scenario.

In order to avoid waste of time, each session and fixed appointment must be limited in time. Each team can dedicate the desired time to the project according to their needs.

To consider continuous learning, in the last episodes of the experience, students can use all the knowledge provided during the path of the master. In this way, they can deepen, review the contents explained previously favouring the storage.

5.14.8 Practical implementation

In 5.2 is represented game and learning elements thanks to the statical table for the experience presented

5.15 Case studied: try hack me advent of cyber

This section has analysed a project that reflects a lot of methodology elements previous presented.

A gamified experience was realised by try hack me platform on the occasion of the beginning of advent [139]. The platform, already presented in the previous chapter, is a gamified website allowing users to learn topics related to security in a fun and free way. It is possible to take part in different missions and rooms, but in particular, for the advent period they organize an advent calendar: every day from December first to Christmas day there is a new challenge for users.

5.15.1 General Elements

The structure of the experience is a wargame, similar to CTF competition for beginner jeopardy style but without adversary competitive and teamwork.

The chosen target has as aim the approach to the platform and the subject for new categories of users or as a deepening for users already involved. The project is also thought of as an introduction to possible work roles in the cybersecurity context. More specifically in the special section are briefly presented different work positions in cybersecurity: penetration tester, security analyst, incident responder, red team, security engineer.

The challenges are created for a beginner audience level, it is available for everyone who would like to learn and challenge himself about cybersecurity topics.

The general learning content could be summarized in categories: Web Exploitation, Network Exploitation, OSINT, Cloud Hacking, Defensive Blue Teaming.

GM	*LM*	*Implementation*	*Usage*
Role Play, Strategy	Reflect, Analyse	Cards, Role	Use the available cards in relation to the role assigned
Levels	Motivation	Experiences and internal complications	Three distinct experiences each with internal steps
Help, Feedback	Guidance, Instructional	Standard lecture, Experts	Standard lecture, private feedback for each group, public feedback for the whole class
Cooperation	Discuss	Teamwork	Internal comparison to the team and works submission
Competition	Observation, Imitation	Between each team	Comparison with other teams' choices
Storytelling	Tasks	Meeting	scenario presentation via storytelling
Status, Collection	Motivation	Locked or unlocked card	Security elements available or blocked during the path underlining progression
Appointment	Responsibility	Scheduled meeting	Pre-organized meeting for all the class in fixed moments

Table 5.2. Work role statical analyses LM-GM

The tools used are different for each challenge but in general, it is possible to use either a virtual machine with all the material needed already uploaded (provided for free with some limitation or without limitation for premium users) or web site specially created for the challenge.

The gamification elements used are:

- **Storytelling**: all challenges have a common thread. Grinch stole Christmas with malicious actions on Santa's information system. The elf Mcskidy must try to settle, she was promoted to Chief Information Security Officer thanks to the work done in the challenge of the year before. It is important to notice the choice of a common Christmas narration usually known to the most and easy to understand also for inexperienced users. On the other hand, it is also present a loyalty element for users who had already participated in the previous years thanks to briefly recalls of past history elements.

- **Rewards**: there are two types of rewards included. The first one is a final reward, the winner will be randomly chosen among users with the highest number of responses obtained throughout the event. The second one is weekly prizes assigned based on weekly challenges and answers completed. Both are assigned without checking the points obtained but the answers and the constancy, this element invites users to better understand topics without focusing on points and motivate daily use of the platform for continuous learning mechanics.

- **Rules**: at the beginning of the challenge are presented rules, how to play indications with a short tutorial and clarification of forbidden actions with related conterminous as elimination from the competition.

- **Appointment mechanics**: each day is uploaded a new challenge, thanks to both weekly rewards and daily new elements is created the appointment game mechanics for the users.

- **The freedom element**: each chapter is standing alone. Users can try to exploit different challenges without following the order presented. The user is free to choose if play and what

to play at. At the same time, users are guided to avoid the sense of loss thanks to both introduction elements and video presentation for each challenge.

5.15.2 Challenges

Each challenge is organized with different elements:

- Storytelling: each chapter is introduced by a brief contextualization of the security issues related to the Grinch story. It reflects the elements noticed by the story characters on the computer system, without cybersecurity technique knowledge, it is only presented the problem encountered. For example, figure 5.1 is reported the Day 1 Story introduction.

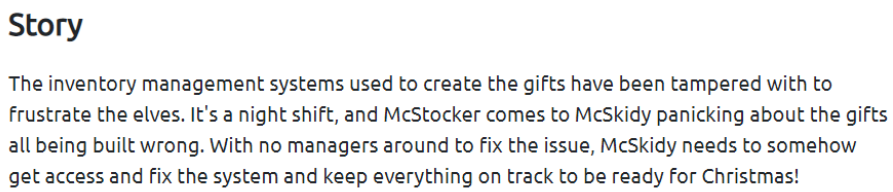

Figure 5.1. Story Day 1 challenge (source: Try Hack Me, Advent of Cyber).

The story is used to introduce the cybersecurity issue that is explained in more technique word and intent in the section after.

- Learning Objectives: for each challenge are listed shortly with cyber elements will be introduced and how the challenge is organized as subsection 5.2.

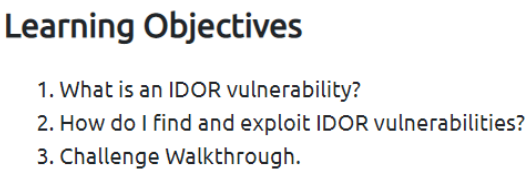

Figure 5.2. Learning Objectives Day 1 challenge (source: Try Hack Me, Advent of Cyber).

The section is composed of the learning object listed before with a brief theoretical explanation, how it is possible to exploit with practical example and, in some cases, link with a real case of attacks and vulnerability, reference to external material or other related mission presented on the platform on the same topics. In the end, the challenge is presented with practical reference to the action that the player has to perform in order to capture all the flags for the related challenge.

- Question and Answers: the last section is dedicated to the answers' boxes. The user can insert his answer and check for correctness thanks to the graphical interface. Each answer requires a precise format as a string or numerical sequence and is specified the precise number or characters required 5.3. From the methodology, it is possible to notice the precision of format answers required to avoid error parsing or evaluation issues.

- Immediate feedback: different graphical elements are used to create feedback. Introducing the answers graphically the user understands if it has solved the problem correctly thanks to a pop-up notification, and to the change of the colour of the control button in green. Once all the questions of the related challenge are completed, the task becomes green 5.4, the unfinished ones remain red 5.5. There is also a general progression bar related to all the advent experiences showing the percentage of completion.

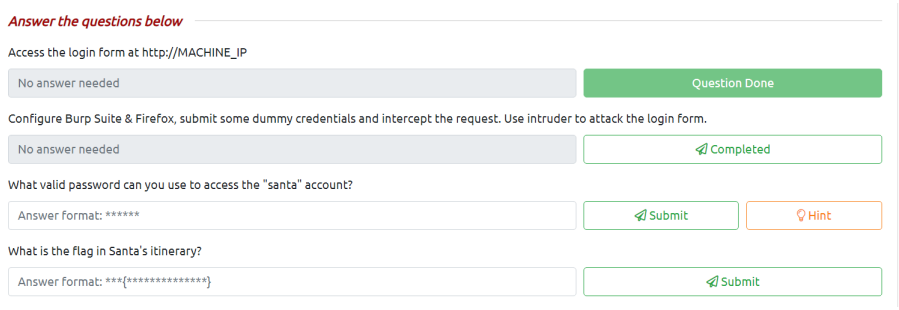

Figure 5.3. Question and Answers Day 4 challenge (source: Try Hack Me, Advent of Cyber).

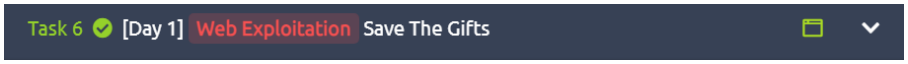

Figure 5.4. Feedback challenge completion Day 1 challenge (source: Try Hack Me, Advent of Cyber).

- Help, for each question it is possible to ask for hints if the user is in trouble 5.3. Throw the graphical interface it is possible to click con the yellow hint button and see a pop-up "Question hint". To ask for a hint does not reduce the answer value but help the player to avoid wasting time and frustration. The hints do not give the solution but little help such as suggested tools or reflection in order to route the user in the right way.

  Other possible help is represented in the introductory video available for each challenge.

- Level, there is not a specific organization with level, but the complexity of the challenge increases slightly with increasing days. On the last days of the challenge are specified some required skills and knowledge as limitations. These prerequisites are not verified from the platform but are presented as information for the user.

  It is also possible to participate in the competition with distinct levels of difficulty self-managed by users. More expert users can solve the question proposed only by reading the challenge presentation and trying by themselves to find the solution, intermediate users can use hints and try to find a solution and beginners can solve the challenge steps by steps following the video instruction.

  In this way it is possible to recognize different elements of Bloom for the Psychomotor for different usage levels: beginner imitation, intermediate manipulation and expert articulation and for advanced naturalisation 5.3.

- Challenge focus on a specific cybersecurity task (es: IDOR, HTTP(S), Cookies, authentication) each time, if some previous knowledge is required in the introductory section it is specified and the user can find a link or material to investigate. In the first chapters, each section is a basic block for security content, in the last sections more than one element and topic can be processed together but every single element has been already presented on a previous distinct day.

  Each challenge focuses on security problems and never on a specific tool. Obviously, some tools, such as Whirshark or BurpSuite, are presented as a means to solve the problem but the focus is not to explain how these tools work. Users are also free to resolve the challenge with outer tools in the private environment.

- The influence factor is mainly personal interest in understanding and extending personal knowledge related to security topics in a more theoretical way.

- Fruition time, the competition itself lasts the 25 days of advent but the performance of individual challenges engages users for 10/15 minutes per day. This element respects the methodology suggestion to demand a small but constant effort in a longer overall duration.

Figure 5.5. Feedback challenge unfinished Day 4 challenge (source: Try Hack Me, Advent of Cyber).

User Level	*Bloom Cognitive level*	*Bloom Psychomotor Level*	*Project element*
Basic	Knowledge, Comprehension	Imitation	Video
Intermediate	Application	Manipulation	Instruction and hints
Advanced	Analysis	Precision, Naturalization	Self resolution

Table 5.3. Cyber advent level analyses

5.15.3 Gamification elements do not use

Some gamification elements are not incorporated into the experience. For example, cooperation is not contemplated and also discouraged to avoid sharing the solutions of the challenges publicly. There is not the possibility to work in a team and exchange on the platform experience and ideas with peers.

The teaching content is meanly passive: video and written content, users in order to learn topics have to read, watch and listen only at the end he can apply practically what is explained verbally.

Points and badges are not used, users can compare its work only by its performance and not comparing other player outcomes.

Levels are not explicitly created but challenges are created with increasing difficulty.

There is no use of avatars or similar object, the user act externally to the story: he is not in the role of one narration character.

5.15.4 Learning content

In the table 5.4 are summarized the learning content of the challenge focused on the main learning object, related content, used tools, knowledge necessary to carry out the activity with, when available, reference to the internal experience unite and category.

The legend used to classify categories is:

- WE = Web Exploitation
- S = Special
- N = Network
- C = Cloud
- BT= Blue Teaming
- PE= Post Exploitation

5.15.5 Practical Implementation Structure

It is possible to analyse the project via the statical LM-GM representation 5.5 and the different levels of use linked with the Bloom elements 5.3.

Table 5.4. Learninggontent Cyber advent

Day	*Learning Object*	*Related Content*	*Tools*	*Prerequisite*	*Category*
1	IDOR Vulnerability	Cookies, URL structure			WE
2	Cookies manipulation	HTTP(S) protocol			WE
3	Content Discovery	folder structure and default credentials	Dirbuster		WE
4	Authentication	Fuzzing	Burp Suite		WE
5	XSS vulnerability	HTML			WE
6	LFI vulnerability	input validation, RCE, HTTP GET& POST, PHP			WE
7	NoSQL injection	JSON	MongoDB	SSH	WE
8	PowerShell Transcription Logging		ShellBags Explorer	Encode	S
9	Packet analysis	HTTP GET/POST, DNS, FTP	Wireshark	TCP, IP, OSI model	N
10	Services	IP, protocol and ports	Nmap		N
11	Relational Database		SQL	Day 10	N
12	Unusual traffic	NFS, MD5		Day 10, SSH	N
13	Privilege escalation	Windows privilege escalation vectors			N
14	CI/CD exploitation vectors	DevOps	Dirbuster	Day 3 and 13, SSH	N
15	Cyber Security Careers Quiz				S
16	OSINT	Account, blockchain hints, ransomware			OSINT
17	Cloud		AWS, Amazon S3		C
18	Docker			Day 16	C
19	Phishing	Encode Base64	CyberChef		BT
20	File Analysis	file type, file hash, find string	VirusTotal		BT
21	Malicious files from network		Yara		BT
22	Encoded, encryption	macro	CyberChef, Oledump		BT
23	Event Logs analysis	PowerShell Scripting	Powershell	Day 19	BT
24	Post exploitation and Password	Password stored and hashes	Mimikatz, Sekurlsa		PE

GM	*LM*	*Implementation*	*Usage*
Story	Introduction	Written story chapter	Introduce cybersecurity issues via storytelling
Rewards	Extrinsic motivator	Weekly and Final prices	Continuous learning and appointment dynamic
Information	Instruction	Written learning content	Guide user by cybersecurity content information
Question and Answer	Action and feedback	Interaction with graphics interface	Verify user knowledge acquisition
Feedback	Feedback and intrinsic motivator	Graphics elements	Psychological rewarding all the small results obtained
Simulation	Experiment, reflect, analyse, discover	Virtual machine, tools, web sites	Practical implementation of the theoretical knowledge
Tutorial	Guidance	Prepender video	help and guidance
Hints and help	Guidance	Interaction with graphics interface	Avoid stress, frustration, wast of time

Table 5.5. Cyber advent Statical analyses LM-GM

Chapter 6

Applications

6.1 Project Work

The first application of our methodology was tested in a university course in Politecnico di Torino called Project Work taken by Professor Atzeni. The final goal is the risk assessment of a simple IoT system previously created by other university students.

6.1.1 Initial ideas

The target considered are students in manufacturing engineering courses, not expert in cybersecurity but with a background in basic security and computer science knowledge. The course was structured with 30 hours of standard lecture and more than 100 hours to work on the project group and deepen the subject.

The gamified elements chosen are:

- Real interaction with tools: professor during lectures presents tools and assigns individual homework. Each student has to work individually and hands over their work to the professor. Each homework is evaluated and kept into account for the final evaluation only if the work assigned is related to the final project.
- Recognition and Comparison: it is created a scoreboard of anonymous homework with the most and the least related works to the assignment. In this way professor analyses correct and incorrect elements for all the class.
- Personalized feedback: professor gives to each work a private comment underlining how to improve the homework and what is already correct. The aim is to motivate the student and to give ideas for improvement.

Table 6.1 are summarized the game and learning mechanics used in the project.

The evaluation considers two metrics:

- Final mark obtained by students
- Personal students' ideas of the experience via a survey related to mechanics used

6.1.2 Actual implementation

In the actual implementation, there was some limitations. The course was in its first edition and some rules are defined during its run. Therefore, previous organization was difficult to manage.

GM	*LM*	*Implementation*	*Usage*
Question and Answer	Task, Experimentation, Imitation, Discovery	Homework	Weekly homework assigned lectures provided
Feedback, Personal rewards/penalty	Competition, Comparison	Public homework, Leaderboard	Anonymous homework comparison
Feedback	Guidance	Personal feedback	Professor homework feedback in a private way

Table 6.1. Project Work statical analyses LM-GM

For these reasons, the gamification approach was limited to the sub-topic of certificate and certification authority.

The gamified experiences were two:

1. Two teams are charged to solve in class a problem presented, using sharing tools, discuss and verify the pros and cons.
2. Individual homework regarding the modelling of each student's home network.

In both cases, non-anonymous intra-group feedback was used. In the first case, were used only verbal feedback in the work open discussion. In the second case was used writing feedback, each student has to comment on the work of a classmate. Professor perception reports that despite the anonymity students were honest, reasonable and constructive, with a view to improvement.

On organization, Professor found it helped to organize both experiences in many mini-tasks and sub-points, which made the differences and the parts on which to give feedback improvements clearer. In general, this specificity could lock in and limits the possibilities, but in a learning phase too open issues could confuse and to go off-road. Perhaps, with students with experience on the topics freer and open questions could lead to different results.

Therefore, respecting the initial ideas there were homework assignments but without anonymization and real tasks leader-board.

6.1.3 Professor's Point of view

Thanks to the experience, the Professor analyses some interesting elements. As a limitation, it is important to underline the difficulty of extrapolating certain results into a context where the activities with gamification have been limited to a few experiences compared to the whole course.

As positive aspects, it is possible to recognise that experiences:

- Allowed an improvement of the team spirit.
- Increased the inclination of student participation during standard lessons. Concerning this, it was fundamental not to give any kind of punitive inclination, both explicit and implicit, to the gamified session.
- Helped Professor understand different gaps and strengths of the students. The gamified approach should also help the professor more easily understand the actual students' degree of learning of concepts. Consequently, it allows introducing correctives during the rest of the course.
- The topic itself has been mentioned several times in the rest of the course, suggesting a great cognitive hook.
- The topic chosen for gamification lessons is usually presented within various security courses. It was chosen also for its usually boring students' perception.

It is possible to recognize other observations thanks to the Professor's experience. The gamification approach is more time consuming compared to the standard education, but the students' learning depth is greater.

Other interesting observations are reported with respect the anonymity and the context. The Professor finds the use of anonymity very useful to hold freedom of expression, but it is to be balanced by considering the context in which you act. The Professor noted that the fundamental thing is that the participants have the confidence to act. If, on the contrary, they fear judgment or, even worse, the possibility of retaliation, then anonymization becomes important to increase trust. However, in the context of Project Work, it was possible to observe a relaxation in the intra-student comparison. It is important to note that the students had already worked together before, and they were close. Regarding the student-teacher comparison, the Professor has personally contributed to creating a non-judgmental environment.

This inclination has involved avoiding a real ranking and leader-board of the worst and best homework but instead dwelling on what were the weaknesses and strengths of homework. This has effectively created team cohesion: everyone has felt that they have participated in the common work, despite the individuality of the homework, allowing everyone to participate. At least each student could explain his criticism recognized on the work of others. It allowed the collection of information on strengths and weaknesses, which was evident in the examination phase. Indeed, the exam presents a similar but larger work, done in the same way as to work on network modelling. The results are improved.

6.1.4 Students' Point of view

In order to evaluate the experiences also students' side, it was created a survey via Google Forms. Instead, the final mark is not kept in consideration because the gamification experiences are limited respect the whole course. The survey was shared with the six students that took part in the project. We obtained five answers. The sample is not statistically relevant, but the observations extracted offer interesting things to consider.

The survey is organized in different sections: comprehension, time, classroom atmosphere and suggestions. It guarantees anonymisation.

The survey created, reported B, is written in Italian because shared with Italian students.

Comprehension

Considering the comprehension almost all students agree on its benefits. The activities perceived as more useful for understanding for all the students there are interaction with shared spreadsheets and class comparison with the Professor. Four of them also select teamwork in class and three of them select Professor correction.

On the other hand, they consider less useful individual homework, peers comparison and peers' correction.

It is interesting that all the students agree that the standard explanation was helpful but proposed gamified activities have made more immediate and simpler the understanding process.

Time

About the time devoted to the experiences all students except one declare that the time has been adequate, instead, a student considers the time available too little.

For the homework, the time to dedicate to it is considered by all the students adequate.

However, all the students have a different point of view concerning the time dedicated to studying the topics presented with gamification for the final exam. One took more time than the topics explained in a standard way, one claims to have devoted the same time and two indicate a shorter time. A student explains:

> The time devoted to the work was a lot. But the topics addressed with gamification were found to be clearer than others.

Classroom atmosphere

In the gamification experience, the classroom atmosphere is fundamental. About all students agree that the atmosphere was enjoyable and conducive to participation in activities. The 100% of students feel involved, 80% focused on the activities and 60% enjoyed and welcomed. Nobody feels embarrassed, boarded or judged.

Regarding participation and involvement, students prefer the comparison with Professor, comparisons with peers, teamwork, and interaction with shared spreadsheets. On the other hand, the less chosen activities are individual homework and Professor correction. Correction between peers has been chosen by no one.

All students experienced the moments of correction as a moment of stimulation and understanding. On the issue of correction, the professor played a key role. A student answers:

> The Professor was always very calm when he corrected us.

Suggestions

For future improvements, students suggest:

- Deepen some topics and organize the time available in a better way.
- From the beginning make clearer students' goals and the general overview of the work.
- Increase lessons hours.

As general observation students appreciate working on little teams (three people for teams):

> The fact of working in teams of a few people has facilitated the understanding of the subject since you felt fully involved.

Students also observed the useful the creation of reusable models. For example, the model used for the home network was reused to start the analysis of the real object of analysis of the course.

6.2 Training and Awareness via Gather

Another application idea designed with the methodology is focused on training and awareness purposes for private users. The idea designed is theoretical and open for future implementation.

6.2.1 Draft Idea

In this case, the focus is on private users' involvement to deepen understanding of cybersecurity issues and how to actively defence themself. The activity tries to find a compromise between COVID-19 limitation and social interaction.

- Skills and topics:

  The target involved is not technical in cybersecurity and computer science. However, they are personally interested in participating and increasing their defence skills in everyday life.

  For these reasons, the topics selected refer to social engineering and take as guidance CAPEC framework. The idea is to explain cybersecurity issues starting from a real case as phishing, identity spoofing, social engineering, software update, remote work, mobile, password. The skills to train are perceived susceptibility, perceived severity, perceived safeguard effectiveness and self-efficacy.

- Tool and technology

  The presented tool is Gather. Gather allows creating maps inside which users can interact with objects and share imagines, videos, text, external links and call zoom. Interaction with other participants is quite similar to a normal video call but each participant is represented as an avatar that can move around the map and interact with other users and objects. This element creates a game context in which users can interact easily.

  Figure 6.1 represent an example of a Gather map with some interactive objects.

Figure 6.1. Gather Map, room example.

Considering the teaching content, it is possible to manage different security issues. Inside the room reported 6.1 it is possible to see different elements that contain clues to solve the specific mission:

  - On the table, there is a form that users have to complete thanks to the information gathered. The aim in answer correctly to as many questions as possible.
  - The board report general information about the security issues.
  - The pirate flag contains the main dangers referred to as security issues of the session.
  - Swords explain how to defence and act to avoid security issues.
  - The newspaper reports real cases of the problem presented.

- Rules:

  The experience aims to answer questions related to specific security issues thanks to the cooperation and hints collections. Users are divided into groups of two. They have to collect information and find the correct solutions. They can ask for help from a supervisor that interacts only when required. Each team has limited time to answer the proposed questions.

- Game elements:

  - Help, participants could ask for moderators for help via chat or video call.
  - Team cooperation for filling the questions' form.
  - Interaction with room's elements and collection of information.

- Fruition time:

  Each security issue is presented in an independent module. One session is characterized by one specific module. Global experience can include multiple modules. Each session should

last about half an hour. The initial idea was to organize one session per week. The user's commitment is about half an hour per week for a maximum of one month.

Chapter 7

Conclusions

This thesis has analysed gamification and its application in cybersecurity fields. In order to propose an alternative to the standard education in cybersecurity to compensate for the main shortcomings highlighted over the years. Thanks to literature reviews, end-users' opinions, experts interviews and experiences it was developed an original methodology that summarizes hints and suggestions in order to create a gamification experience in a cybersecurity environment.

As for the strengths points of the work, it is possible to recognize the analyse of a heterogeneous source of information and the proposal of a methodology applicable in all contexts: both technical and non-technical. The methodology puts the focus of attention on the end-users considering different goals and purposes of application in relation to different targets and usage but always related to security education. The work aims to respond to a real and current need: to improve and extend to the widest possible public knowledge in cybersecurity, considering different levels of depth of content.

The work proposes in a practical way how to use the methodology both to create a gamification experience and both to analyse already existing one. Indeed, the work proposes a possible experience in the technical education environment and an analysis of the already existing application in the private sector.

7.1 Future works

To continue and improve the work presented is possible to identify some areas of interest as potential future works:

- First of all, it will be interesting to practically apply the theoretical experience proposed in the previous chapter. Thanks to the practical implementation it will be easier to recognise straights and limits both of methodology proposed and the application thought.
- Consequentially, the actual application will lead to concrete feedback both related to the organization and the use. The methodology will be modified and increased thanks to the actual results obtained and real feedback acquired.
- On the other hand, a field of possible further investigation is the work environment. In the work context will be possible to collect more information from companies and employees that already use gamification in training and awareness sessions and education. The information gathered will be used to implement the methodology specifically related to the work environment.
- In the same context of analysis, it will be possible to propose a new gamification experience and apply it in a real context. Continuing with the idea of deepening the methodology thanks to real feedback following actual applications.

- Another possible future investigation concerns the recognition of new categories interested in cybersecurity education not represented by categories proposed from work such as children and the elderly.

Appendix A

End-Users Survey

Sicurezza informatica e gamification

Ciao, sono Chiara, studentessa del Politecnico di Torino. Sto lavorando alla mia tesi a conclusione della laurea magistrale in ingegneria informatica e avrei bisogno del vostro aiuto! Sto indagando sulla formazione in campo sicurezza informatica (principalmente per NON tecnici in QUALSIASI ambito lavorativo) con il fine di capirne i principali limiti e poterla migliorare per creare un'esperienza lavorativa motivante e coinvolgente anche, e soprattutto, rispetto a tematiche che magari non sono proprio il nostro principale interesse 😉

Tutti oggi accediamo regolarmente ad internet e utilizziamo la tecnologia per svolgere le nostre attività quotidiane (lavorative o meno). Circa il 90% degli attacchi informatici hanno come origine un errore umano. La formazione è sicuramente un tassello importante per tutelare noi stessi e il nostro lavoro.

Perché ho bisogno del vostro aiuto? Credo che sia importante mettere al centro della mia ricerca l'utente (potenzialmente non tecnico in campo sicurezza) con le proprie esperienze ed idee per poter creare una metodologia di formazione più utile ed efficace possibile.

Potrete lasciarmi vostri commenti che descrivano le vostre esperienze o idee in merito. I dati raccolti garantiscono l'anonimato, se invece siete interessati all'argomento sarò felice di condividere i risultati del mio lavoro: nell'ultima sezione potete lasciami un vostro contatto.
Se una volta completato il sondaggio avete voglia di condividerlo con amici e conoscenti ve ne sarei grata 😊
Giuro, il sondaggio richiede al massimo due minuti 😊
Grazie!

*Campo obbligatorio

1. Quanti anni hai? *

Contrassegna solo un ovale.

- ◯ <18
- ◯ 18-25
- ◯ 25-35
- ◯ 35-45
- ◯ 45-55
- ◯ >55

2. In quale ambito lavori o studi? *

_____

3. In generale, ritieni che la sicurezza informatica sia importante e ti riguardi in prima persona? *

Contrassegna solo un ovale.

- ◯ No
- ◯ Sì, ma non posso agire in prima persona
- ◯ Sì, ma non è rilevante per la mia attività
- ◯ Sì
- ◯ Altro: _____

4. Hai mai seguito corsi di formazione sulla sicurezza informatica (phishing, protezione dei dati, password, regole di comportamento...)? *

Contrassegna solo un ovale.

- ◯ Sì
- ◯ No *Passa alla domanda 15.*

Se hai seguito un corso sulla sicurezza informatica

La tua esperienza

5. Come è stato fruito il corso? *

Contrassegna solo un ovale.

- ◯ La tua interazione è stata principalemente passiva (hai ascoltato o letto le linee guida presentate)
- ◯ La tua interazione è stata principalmente attiva (video interattivi, esperienze ludiche, simulazioni)

6. In quale misura il corso è stato fruito da remoto? *

Contrassegna solo un ovale.

- ◯ 100% (Interamente da remoto)
- ◯ 70%
- ◯ 50%
- ◯ 20%
- ◯ 0% (Interamente in presenza)

7. In quale misura il corso ha previsto esperienze e attività di gruppo? *

Contrassegna solo un ovale.

- ◯ 100% (corso interamente organizzato con attività di gruppo)
- ◯ 70%
- ◯ 50%
- ◯ 20%
- ◯ 0% (nessuna attività di gruppo)

8. In caso di esperienze attive (video interattivi, esperienze ludiche, simulazioni) i tuoi risultati sono stati riassunti in punteggi? *

Contrassegna solo un ovale.

- ◯ Sì
- ◯ No
- ◯ Esperienza passiva
- ◯ Altro: _____

9. In caso di esperienze attive (video interattivi, esperienze ludiche, simulazioni) i tuoi risultati sono stati messi a confronto con altri utenti/colleghi? *

Contrassegna solo un ovale.

- ◯ Sì
- ◯ No
- ◯ Esperienza passiva
- ◯ Altro: _____

10. Ci sono altri elementi caratteristici della tua formazione che hai piacere di condividere?

_____

_____

_____

_____

_____

11. Con che frequenza segui formazione e aggiornamento in ambito di sicurezza? *

Contrassegna solo un ovale.

- ◯ Ho seguito un corso una volta sola
- ◯ Una volta all'anno
- ◯ Più volte all'anno
- ◯ Altro: _____

12. Se hai riscontrato difficoltà durante la fruizioni, quali sono state? *

Seleziona tutte le voci applicabili.

- [ ] Difficoltà nel comprendere concetti prettamente teorici, tecnici e spesso astratti
- [ ] Difficoltà nel capire come poter agire attivamente per la sicurezza personale e aziendale
- [ ] Difficoltà nel mettere in atto i consigli ricevuti
- [ ] Nessuna difficoltà
- [ ] Altro: _____

13. Come ti sei sentito durante la fruizione del corso? *

Contrassegna solo un ovale.

- ◯ Non mi interessava, l'ho vissuta come uno spreco di tempo
- ◯ Non mi interessava, ma ne ho percepito l'utilità nella mia vita quotidiana lavorativa e personale
- ◯ Ne ero interessato personalmente, ma non so come applicare le conoscenze apprese nella vita di tutti i giorni
- ◯ Ne ero interessato e l'ho trovato utile
- ◯ Altro: _____

14. Grazie alle nozioni acquisite, la tua consapevolezza e i tuoi comportamenti quotidiani rispetto alla sicurezza informatica sono cambiati? Se sì, come?

_____

_____

_____

_____

_____

Elementi di gioco

La gamification utilizza elementi nativi del gioco in contesti non ludici, se si potesse applicare nella formazione in ambito sicurezza informatica...

15. Ti piacerebbe rendere la formazione più coinvolgente con l'introduzione di elementi di gioco, anche in un contesto serio come quello lavorativo? *

Contrassegna solo un ovale.

- ◯ Sì
- ◯ No

16. Se si potesse far diventare la formazione più divertente e motivante, quali elementi del mondo del gioco non potrebbero mancare per te? *

Seleziona tutte le voci applicabili.

- ☐ Competizione tra colleghi
- ☐ Competizione tra team
- ☐ Racconto e elementi narrativi
- ☐ Collezione, ricerca di elementi
- ☐ Interazione fisica con strumenti
- ☐ Feedback immediati
- ☐ Ricompense, riconoscimenti
- ☐ Socializzazione e cooperazione tra colleghi e team
- Altro: ☐ _____

17. Se si potesse far diventare la formazione più divertente e motivante, quali elementi del mondo del gioco NON vorresti venissero introdotti nell'ambiente lavorativo? *

Seleziona tutte le voci applicabili.

- ☐ Competizione tra colleghi
- ☐ Competizione tra team
- ☐ Racconto e elementi narrativi
- ☐ Collezione, ricerca di elementi
- ☐ Interazione fisica con strumenti
- ☐ Feedback immediati
- ☐ Ricompense, riconoscimenti
- ☐ Socializzazione e cooperazione tra colleghi e team
- Altro: ☐ _____

18. Hai voglia di motivare brevemente gli elementi scelti o scartati precedentemente?

19. Conoscere casi reali di attacchi/vulnerabilità nel tuo ambito specifico ti motiverebbe nell'avvicinarti alla sicurezza informatica, sentendolo più vicina alla tua realtà? *

Contrassegna solo un ovale.

- ◯ Sì
- ◯ No
- ◯ Altro: _____

20. Hai altri commenti o riflessioni rispetto alla sicurezza informatica che ti farebbe piacere condividere?

Conclusione

La mia e-mail è chiara.oggeribreda@gmail.com, se hai piacere di ricevere maggiori informazioni sono a disposizione!

21. Se hai piacere di rimanere aggiornato sui risultati della mia ricerca, puoi lasciarmi un tuo contatto!

Appendix B

Students Project Work Survey

Project Work

Ciao, sono Chiara, studentessa del Politecnico di Torino. Sto lavorando alla mia tesi a conclusione della laurea magistrale in ingegneria informatica ed il Professore Atzeni è il mio tutor.
L'argomento della mia tesi è l'utilizzo di elementi di gioco (gamification) in ambito d'insegnamento della sicurezza informatica.

Una piccola parte del vostro corso "Project Work" è stato organizzato tenendo in considerazione alcuni elementi di gioco. In particolare 1) le lezioni su certificati e certification authority che hanno incluso: attività di lavoro in gruppo, interazione con tools, e 2) gli homework sulla modellazione della rete di casa, feedback e discussione in aula, correzioni tra pari e non. Avrei, quindi, piacere di raccogliere vostre osservazioni in merito.

Il sondaggio è ovviamente anonimo, vi ringrazio molto per la partecipazione :)

*Campo obbligatorio

Comprensione

1. Rispetto alle lezioni ed esperienze proposte con gamification ritieni che siano state in generale utili per la comprensione degli argomenti proposti? *

Contrassegna solo un ovale.

	1	2	3	4	5	
Completamente d'accordo	◯	◯	◯	◯	◯	Per niente d'accordo

2. Quali attività con gamification hai ritenuto MAGGIORMENTE utili per la comprensione degli argomenti? *

Seleziona tutte le voci applicabili.

- [ ] Lavoro in team in classe
- [ ] Utilizzo di strumenti e tools
- [ ] Homework individuale
- [ ] Confronto in classe con il Professore
- [ ] Confronto tra pari
- [ ] Correzione Professore
- [ ] Correzione tra pari
- [ ] Altro: _____

3. Quali attività con gamification hai ritenuto MENO utili per la comprensione degli argomenti? *

Seleziona tutte le voci applicabili.

- [ ] Lavoro in team in classe
- [ ] Utilizzo di strumenti e tools
- [ ] Homework individuale
- [ ] Confronto in classe con il Professore
- [ ] Confronto tra pari
- [ ] Correzione Professore
- [ ] Correzione tra pari
- [ ] Altro: _____

4. La comprensione dell'argomento proposto con modalità attiva... *

Contrassegna solo un ovale.

- ◯ Era chiaro anche solo con la spiegazione teorica standard (lezione frontale)
- ◯ La spiegazione standard è stata utile ma attività proposte hanno reso più immediato e semplice la comprensione
- ◯ L'argomento è stato di difficile comprensione sia durante la spiegazione standard sia con le attività proposte
- ◯ Altro: _____

Il tempo

5. Il tempo dedicato alle esperienze proposte in classe è stato adeguato? *

Contrassegna solo un ovale.

- ◯ Il tempo a disposizione è stato troppo poco
- ◯ Il tempo a disposizione è stato adeguato
- ◯ Il tempo a disposizione è stato troppo
- ◯ Altro: _____

6. Il tempo necessario per completare le esperienza individuali a casa è stato: *

Contrassegna solo un ovale.

- ◯ Troppo
- ◯ Adeguato
- ◯ Poco
- ◯ Altro: _____

7. Considerando l'argomento proposto con gamification e la preparazione all'esame finale, quanto tempo hai dovuto dedicare allo studio? *

Contrassegna solo un ovale.

- ◯ Più tempo rispetto agli argomenti spiegati in modo standard
- ◯ Lo stesso tempo degli argomenti spiegati in modo standard
- ◯ Meno tempo degli argomenti spiegati in modo standard
- ◯ Nessun tempo di studio aggiuntivo, oltre alla frequentazione delle lezioni
- ◯ Altro: _____

8. Oggi, dopo circa un mese dall'esame, qual è l'argomento del corso che ricordi con maggior facilità? *

_____

Il clima in aula

9. Ritieni che il clima creato in classe sia stato adeguato ad incentivare in modo corretto e piacevole la partecipazione alle attività proposte? *

Contrassegna solo un ovale.

	1	2	3	4	5	
Completamente d'accordo	◯	◯	◯	◯	◯	Per niente d'accordo

10. Quali attività proposte hai accolto con maggior interesse in termini di partecipazione e coinvolgimento? *

Seleziona tutte le voci applicabili.

- [ ] Lavoro in team in classe
- [ ] Utilizzo di strumenti e tools
- [ ] Homework individuale
- [ ] Confronto in classe con il Professore
- [ ] Confronto tra pari
- [ ] Correzione Professore
- [ ] Correzione tra pari
- [ ] Altro: _____

11. Come ti sei sentito durante le attività proposte? *

Seleziona tutte le voci applicabili.

- [ ] Divertito
- [ ] Partecipe
- [ ] Concentrato
- [ ] Accolto
- [ ] Imbarazzato
- [ ] Annoiato
- [ ] Giudicato
- [ ] Altro: _____

12. Come hai vissuto i momenti di correzione e feedback? *

_____

Suggerimenti

13. Al fine di migliorare l'esperienza vissuta, cosa modificheresti?

14. Hai altri suggerimenti o osservazioni che hai piacere di condividere sull'esperienza?

Bibliography

[1] "Rapporto Clusit 2021 sulla sicurezza ICT in Italia", Clusit, March 2021, (Italian)

[2] ProofPoint, "Human Factor report 2019", 2019, https://www.proofpoint.com/

[3] Maddie Rosenthal, "Must-Know Phishing Statistics: Updated 2021", Tessian, Sept 2021, https://www.tessian.com/blog/phishing-statistics-2020/

[4] Rob Sobers, " 64% of Americans Don't Know What to Do After a Data Breach. Do You? (Survey)", Veronis, 2020, https://www.varonis.com/blog/data-breach-literacy-survey/

[5] D. Wu, G.D. Moody, J. Zhang, P.B. Lowry, "Effects of the design of mobile security notifications and mobile app usability on users' security perceptions and continued use intention", Jul 2020, DOI 10.1016/j.im.2019.103235

[6] Kaspersky, "What is Smishing and How to Defend Against it", 2021, https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

[7] World economic forum and Accenture, "Global Cybersecurity Outlook 2022", Jen 2022, https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

[8] Alliantgroup Company, "Small businesses, the flight to remote working cybersecurity report", 2021, https://www.alliantcybersecurity.com/wp-content/uploads/2020/05/alliant-cybersecurity-Remote-Working-Report-2.pdf

[9] IC3, "2020 Internet Crime Report", 2020, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[10] IBM security, "Cost of a Data Breach Report 2021", Jul 2021, https://www.ibm.com/downloads/cas/OJDVQGRY

[11] NetSec, "2018 Security Awareness Training Statistics", NetSec.news Dec 2018, https://www.netsec.news/2018-security-awareness-training-statistics/

[12] L. Spitzner, "Top 3 Reasons Security Awareness Training Fails", SANS Jen 2019, https://www.sans.org/blog/top-3-reasons-security-awareness-training-fails/

[13] Annie Velev, "Zombies Level Up Fitness Gamification", Feb 2016, http://www.megamification.com/zombies-level-up-fitness-gamification/

[14] Marco Segatto, "Nike SNEAKRS Day", Aug 2019, https://www.projectfun.it/case-studies/nike-sneakrs-day/ (Italian)

[15] J. Bilham, "Case study: How Duolingo Utilises Gamification to Increase User Interest", Jul 2021, https://raw.studio/blog/how-duolingo-utilises-gamification/

[16] P. Noorata, "Children's Hospital's Fantastic Pirate-Themed CT Scanner", Aug 2013, https://mymodernmet.com/morgan-stanley-children-s-hospital-of-newyork-presbyterian/

[17] M. Moore, "Bringing Gamification to Cyber Security Training", University of San Diego, https://onlinedegrees.sandiego.edu/bringing-gamification-to-cyber-security-training/

[18] Infosec, "Gamification: Making cybersecurity training fun for everyone", InfoSec, 2021, https://www.infosecinstitute.com/podcast/gamification-making-cybersecurity-training-fun/

[19] M.Silic, P.B.Lowry, "Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance", March 2020, DOI 10.1080/07421222.2019.1705512

[20] S.Ros, S.Gonzalez, A.Robles, L.L.Tobarra, A.Caminero, J.Cano, "Analyzing Students' Self-Perception of Success and Learning Effectiveness Using Gamification in an Online Cybersecurity Course", May 2020, DOI 10.1109/ACCESS.2020.2996361

[21] W. Ronnie, "Space Shelter, the game that teaches you how to protect yourself online", 2021, https://techgameworld.com/space-shelter-the-game-that-teaches-you-how-to-protect-yourself-online/
[22] A.Marczewski, "Flow, Player Journey and Employee Satisfaction", November 2012, https://www.gamified.uk/2012/11/30/flow-and-satisfaction/
[23] K.Cherry, "Self-Determination Theory and Motivation", March 2021 https://www.verywellmind.com/what-is-self-determination-theory-2795387
[24] R.M.Ryan, E.L.Deci, "Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions", 2000, DOI 10.1006/ceps.1999.1020
[25] R.Landers, "Developing a Theory of Gamified Learning: Linking Serious Games and Gamification of Learning", April 2015, DOI 10.1177/1046878114563660
[26] B.J. Fogg, "Fogg Behavior Model", https://behaviormodel.org/
[27] B.J.Fogg, "A Behavior Model for Persuasive Design", April 2009, DOI 10.1145/1541948.1541999
[28] C.Ruhl, "Bloom's Taxonomy of Learning", May 2021, www.simplypsychology.org/blooms-taxonomy.html
[29] Y.Chou, "Yu-kai Chou: Gamification and Behavioral Design", 2020, https://yukaichou.com/gamification-examples/octalysis-complete-gamification-framework/
[30] S.A.A.Freitas, A.R.T.Lacerda, P.M.R.O.Calado, T.S.Lima, E.D.Canedo, "Gamification in Education: A Methodology to Identify Student's Profile", October 2017, DOI 10.1109/FIE.2017.8190499
[31] R.Hunicke,M.LeBlanc,R.Zubek, "MDA: A Formal Approach to Game Design and Game Research", https://www.aaai.org/Papers/Workshops/2004/WS-04-04/WS04-04-001.pdf
[32] F.Viola, "Gamification MDA Framework", October 2011, https://www.gameifications.com/gamification-mda-framework/ (Italian)
[33] I.P.Santana, "Gamification - The 6D Framework", June 2013, http://useragiledevelopment.blogspot.com/2013/06/gamification-6d-framework.html
[34] G.F. Tondello, A.Mora, A.Marczewski, L.Nacke, "Empirical Validation of the Gamification User Types Hexad Scale in English and Spanish", October 2018, DOI 10.1016/j.ijhcs.2018.10.002
[35] A.Marczewski, "Marczewski's Player and User Types Hexad", October 2018, https://www.gamified.uk/user-types/
[36] A.Marczewski, "The EEEE User Journey Framework", September 2014, https://www.gamified.uk/2014/04/30/eeee-user-journey-framework/
[37] F. Escribano, "Gamification Model Canvas Evolution for Design Improvement: Player Profiling and Decision Support Models", January 2010, https://gecon.es/wp-content/uploads/2017/07/GMC-Evolution_vDef.pdf
[38] F. Escribano, J.M. Gali, "Gamification Model Canvas Framework. Evolution", January 2015, https://gecon.es/gamification-model-canvas-framework-evolution-1/
[39] A. AlMarchiedi, G.B. Wills, V. Wanick, A.Ranchhod, "SGI: A Framework for Increasing the Sustainability of Gamification Impact", June 2015, DOI 10.20533/iji.1742.4712.2015.0123
[40] F.Viola, V.I.Cassone, "L'arte del Coinvolgimento. Emozioni e stimoli per cambiare il mondo", Ulrico Hoepli Milano, 2017, ISBN:978-8820378271 (Italian)
[41] G.Zichermann, C.Cunningham, "Gamification by Design", O'Reilly Media, 2011, ISBN: 978-1449397678
[42] E.Parisi, M.Segatto, "Come ricompensare in modo efficace le persone?", January 2021, https://www.projectfun.it/podcast/come-ricompensare-in-modo-efficace-le-persone-1-2/ (Italian)
[43] Sergio Ligato, "Cos'è engagement Deck?", July 2020, https://www.gameifications.com/gamification-deck-di-fabio-viola/ (Italian)
[44] Fabio Viola, Project Fun, Marketing Toys, "Play-able cards", September 2021, https://playablecards.com/ (Italian)
[45] S. Arnab, T. Lim, M. B. Carvalho, F. Bellotti, S. de Freitas, S. Louchart, N. Suttie, R. Berta, A. De Gloria, "Mapping Learning and Game Mechanics for Serious Games Analysis", 2015, DOI 10.1111/bjet.12113
[46] A.Marczewski, "52 Gamification Mechanics and Elements", Febrauary 2019, https://www.gamified.uk/user-types/gamification-mechanics-elements/

[47] M.Sailer, L.Homner, "The Gamification of Learning: a Meta-analysis", August 2019, DOI 10.1007%2Fs10648-019-09498-w

[48] A. M.Toda, W.Oliveira, A.C.Klock, P.T.Palomino, M.Pimenta, I.Gasparini, L.Shi, I.Bittencourt, S.Isotani, A.I.Cristea, "A Taxonomy of Game Elements for Gamification in Educational Contexts: Proposal and Evaluation", 2019 IEEE 19th International Conference on Advanced Learning Technologies (ICALT), Maceio, Brazil, July 15-18 2019, DOI 10.1109/ICALT.2019.00028

[49] E.Villegas, D.Fonseca, E.Pena, P.Bonet, S.Ferandez-Guinea, "Qualitative Assessment of Effective Gamification Design Processes Using Motivators to Identify Game Mechanics", August 2019, DOI 10.3390/s21072556

[50] M.Sailer, J.Hense, H.Mandl, M.Klevers, "Psychological Perspectives on Motivation through Gamification", https://mediatum.ub.tum.de/doc/1222424/file.pdf

[51] E.Parisi, "L'ABC delle Progress Bar", September 2018, https://www.projectfun.it/game-techniques/dietro-le-quinte-delle-progress-bar/ (Italian)

[52] E.Parisi, M.Segatto "Effetto Zeigarnik nel marketing", October 2020, https://www.projectfun.it/game-techniques/dietro-le-quinte-delle-progress-bar/ (Italian)

[53] J.C.Nunes, X. Dreze, "The Endowed Progress Effect: How Artificial Advancement Increases Effort", March 2006, http://msbfile03.usc.edu/digitalmeasures/jnunes/intellcont/Endowed%20Progress%20Effect-1.pdf

[54] B.Hanssen "The four freedoms of games and gamification", January 2017, https://www.puzzel.com/2017/01/20/four-freedoms-games-gamification/

[55] Design Playground "The Fun Theory", January 2013, http://www.designplayground.it/2013/05/the-fun-theory/

[56] "PlayableCity", https://www.playablecity.com/

[57] M. Bada, A. M. Sasse, J. R. C. Nurse, "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?", Jan 2019, https://arxiv.org/abs/1901.02672

[58] J.R.C.Nurse, S.Creese, M.Goldsmith, "Guidelines for usable cybersecurity: Past and present", October 2011, DOI 10.1109/CSS.2011.6058566

[59] A. Nagarajan, J. M. Allbeck, A. Sood and T. L. Janssen, "Exploring game design for cybersecurity training", 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2012, DOI 10.1109/CYBER.2012.6392562

[60] B. Wolfenden, "Gamification as a winning cyber security strategy", Computer Fraud & Security Nov 2021, DOI 10.1016/S1361-3723(19)30052-1

[61] Infosec, "Gamification: Making cybersecurity training fun for everyone", Feb 2021, https://www.infosecinstitute.com/podcast/gamification-making-cybersecurity-training-fun/

[62] Terranova security "5 Reasons Why You Need Gamification In Your Cyber Security Awareness Program", Set 2021, https://terranovasecurity.com/reasons-you-need-gamification-in-security-awareness/

[63] A. Apostolopoulos, "The 2019 Gamification at Work Survey", talent LMS Aug 2019, https://www.talentlms.com/blog/gamification-survey-results/

[64] C.J.Costa, M.Aparicio, "Gamification Usage Ecology", August 2017, DOI 10.1145/3121113.3121205

[65] C.Bedell, "How gamification can improve employee cybersecurity compliance", InfoSecurity Professional Magazine, July/August 2019, https://www.isc2.org/-/media/ISC2/Member-Resources/Infosecurity-Professional-Magazine/2019/July-Aug-Files/InfoSecurityProfessional_July-August-2019_r-2.ashx?la=en&hash=1FE65338564A58CA75BE576033B5ED31C25A4713

[66] I.Rieff, "Systematically Applying Gamification to Cyber Security Awareness Trainings", March 2018,

[67] E.G.B.Gjertsen, E.A.Gjære, M.Bartnes, W.R.Flores, "Gamification of Information Security Awareness and Training", DOI 10.5220/0006128500590070

[68] J.Hill-Wilson, "6 Ways To Supercharge Your Microlearning Program", June 2020, https://elearningindustry.com/supercharge-microlearning-program

[69] A.Sengirbayeva, M.Sedova, "Why Data-driven Personalized Journeys Are The Future Of Security Training", RSA Conference 2019, San Francisco (USA), March

4-8, 2019, https://www.rsaconference.com/Library/presentation/USA/2019/why-data-driven-personalized-journeys-are-the-future-of-security-training

[70] B.Schneider, N.Bontempo, P.M.Asprion, A.Habbabeh, "Storytelling and Gamification in E-Learning An Empirical Study to Educate Swiss Microenterprises in Data Protection", Technology, Innovation and Industrial Management Online conference, May 20-22, 2020,

[71] O.Glassey, J.H. Morin, "Design Thinking and Storytelling in eGovernment: The Case of ThinkData.ch", ECEG 2013 Como (Italy), Jun 2013, https://hal.archives-ouvertes.fr/hal-00952741

[72] O.Arsenijevic, D.Trivan, M.Milosevic, "Storytelling as a modern tool of construction of information security corporate culture", October-December 2016, DOI 10.5937/ekonomika1604105A

[73] Abu-Amara, F. Almansoori, R. Alharbi, "A novel SETA-based gamification framework to raise cybersecurity awareness", Aug 2021, DOI 10.1007/s41870-021-00760-5

[74] A.Zarreha, C.Saygin, H.Wan, Y.Lee, A.Bracho, "A game theory based cybersecurity assessment model for advanced manufacturing systems", Aug 2018, DOI 10.1016/j.promfg.2018.07.162

[75] S. Hart, A. Margheri, F. Paci, V. Sassone, "Riskio: A Serious Game for Cyber Security Awareness and Education", April 2020, DOI 10.1016/j.cose.2020.101827

[76] R.N.Landers, A.K.Landers, "An Empirical Test of the Theory of Gamified Learning: The Effect of Leaderboards on Time-on-Task and Academic Performance", Jenuary 2015, DOI 10.1177/1046878114563662

[77] D.Frison, A.Surian, "Come incoraggiare Data Security Awareness Il caso del progetto Edu4Sec", 2018, DOI 10.30557/QW000006 (Italian)

[78] K.Boopathi, S.Sreejith, A.Bithin, "Learning Cyber Security Through Gamification", April 2015, DOI 10.17485/ijst/2015/v8i7/67760

[79] Yanick Fratantonio, "Mobisec", 2020, https://mobisec.reyammer.io/

[80] V. Svabensky, J. Vykopal, M. Cermak, M. Lastovicka, "Enhancing Cybersecurity Skills by Creating Serious Games", 2018, DOI 10.1145/3197091.3197123

[81] J. Vykopal, R. Oslejsek, P. Celeda, M. Vizvary, D. Tovarnak, "KYPO Cyber Range: Design and Use Cases", 2018, DOI 10.5220/0006428203100321

[82] A. Antonaci, R. Klemke, C.M. Stracke, M. Spatafora, K. Stefanova, M. Specht, "Gamification to Empower Information Security Education", 2017, https://www.researchgate.net/publication/317586620_Gamification_to_Empower_Information_Security_Education

[83] Techstry, "Space Shelter: a game to increase cybersecurity", Oct 2021, https://www.techstry.net/space-shelter-a-game-to-increase-cybersecurity/

[84] Try To Hack Me, "About Us", 2018, https://tryhackme.com/about

[85] Euroean Cyber Security Month, "Join us in October for #CyberSecMonth 2021 #ThinkB4UClick", October 2021, https://cybersecuritymonth.eu/

[86] K. Yonemura, J.Sato, R. Komura, M. Matsuoka, "Practical Security Education on Combination of OT and ICT using Gamification Method", April 2018, DOI 10.1109/E-DUCON.2018.8363305

[87] M. Gondree, Z.N.J. Peterson, "Valuing Security by Getting [d0x3d!] Experiences with a network security board game", Aug 2013, https://www.usenix.org/conference/cset13/workshop-program/presentation/gondree

[88] T. Denning, A. Lerner, A. Shostack, T. Kohno, "Control-Alt-Hack: The Design and Evaluation of a Card Game for Computer Security Awareness and Education", Nov 2013, DOI 10.1145/2508859.2516753

[89] A. Shostack, "Elevation of Privilege: Drawing Developers into Threat Modeling", Aug 2014, https://www.usenix.org/conference/3gse14/summit-program/presentation/shostack

[90] S. Madessis, H. Goffin, "Another spin to Gamification: how we used Gather.town to build a (great!) Cyber Security Game", Nov 2021, https://blog.nviso.eu/2021/11/09/

[91] V. Schiffer, "How To Gamify Cyber Security At Your Workplace By Running a Cyber Scavenger Hunt", Nov 2020, https://medium.com/seek-blog/how-to-gamify-cyber-security-at-your-workplace-3f3b9238a6ca

[92] A. Kay, "Cyber Scavenger Hunt", https://github.com/arthurakay/cyberscavengerhunt
[93] M. Galikova, V. Svabensky, J. Vykopal, "Toward Guidelines for Designing Cybersecurity Serious Games", 2021, DOI 10.1145/3408877.3439568
[94] N. M. Katsantonis, I. Kotini, P. Fouliras, I. Mavridis, "Conceptual Framework for Developing Cyber Security Serious Games", April 2019, DOI 10.1109/EDUCON.2019.8725061
[95] M. Katsantonis, I. Mavridis, "Ontology-Based Modelling for Cyber Security E-Learning and Training", Nov 2019, DOI 10.1007/978-3-030-35758-0_2
[96] CAPEC "Common Attack Pattern Enumeration and Classification (CAPEC)", https://capec.mitre.org/
[97] M. Lockheed, "Cyber Kill Chain", https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
[98] National initiative for cybersecurity careers and studies, "Workforce Framework for Cybersecurity (NICE Framework)", https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework
[99] M.N.Katsantonis, I.Mavridis, D.Gritzalis, "Design and Evaluation of COFELET-based Approaches for Cyber Security Learning and Training", june 2021, DOI 10.1016/j.cose.2021.102263
[100] H. Alqahtani, M. Kavakli-Thorne, "Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness (CybAR)", Jan 2020, DOI 10.3390/info11020121
[101] M. Khader, M. Karam, H. Fares, "Cybersecurity Awareness Framework for Academia", 2021, DOI 10.3390/info12100417
[102] D. P. D. Rajendran, R. Sundarraj, "An e-ADR (elaborated Action Design Research) Approach Towards Game-based Learning in Cybersecurity Incident Detection and Handling", 2020, DOI 10.24251/hicss.2020.623
[103] A.Mavroeidi, A.Kitsiou, C.Kalloniatis, S.Gritzalis, "Gamification vs. Privacy: Identifying and Analysing the Major Concerns", March 2019, DOI 10.3390/fi11030067
[104] T.W.Kim, K. Werbach, "More than just a game: ethical issues in gamification", May 2016, DOI 10.1007/s10676-016-9401-5
[105] livingsecurity, "Cyber Security Top 10 Best Games To Make Your Employees Aware", https://www.livingsecurity.com/10-best-cyber-security-games-for-employees?fbclid=IwAR1IYpDjhP84kLGNJEpXLCfui8rAYB1PODZsl9wMKINsS0UFiMMtZOCB4BA
[106] Texas A&M University, "Keep Traditional Secure", 2010, https://keeptraditionsecure.tamu.edu/
[107] pwc, "Game of Threats", 2020, https://www.pwc.com/lk/en/services/consulting/cybersecurity/game-of-threats.html
[108] The Fugle Company, "Targeted attack: the game", 2015, http://targetedattacks.trendmicro.com/
[109] D.Arnold, "Zero Threat: How we did it", 2017, https://preloaded.com/blog/insight/zero-threat-how-we-did-it/
[110] Preloaded, "Zero Threat The dangerous forces of cybercrime are simulated in this tense, turn-based training game for corporate employees.", 2017, https://preloaded.com/work/preloadedeukleia-zero-threat/
[111] Living Security, "Craft A Phish", https://phishing.livingsecurity.com/
[112] Living Security, "Living Security Teams: CyberEscape Online", https://www.livingsecurity.com/cyberescape-online
[113] Enisa, "Capture-The-Flag Competitions: all you ever wanted to know!", May 2021, https://www.enisa.europa.eu/news/enisa-news/capture-the-flag-competitions-all-you-ever-wanted-to-know
[114] CTF Time, "What is Capture The Flag?", https://ctftime.org/ctf-wtf/
[115] N. Ahmed, "Strategies To Win A CTF: How To Approach A Jeopardy Style CTF", Aug 2020, https://www.cybrary.it/blog/strategies-to-win-a-ctf-how-to-approach-a-jeopardy-style-ctf/
[116] Reply, "CYBER SECURITY CHALLENGE 2021 Powered by Reply and Sponsored by Intesa Sanpaolo", 2021, https://www.reply.com/en/newsroom/events/cyber-security-challenge21

[117] D.Antonioli, H.R. Ghaeini, S.Adepu, M.Ochoa, N.O.Tippenhauer, "Gamifying Education and Research on ICS Security: Design, Implementation and Results of S3 ", 2017, https://arxiv.org/abs/1702.03067
[118] CyberChallenge, "We train the next generation of Cyberdefender", 2017, https://cyberchallenge.it/
[119] ImmersiveLabs, "Learning like hackers to stay ahead of the game", 2021, https://www.immersivelabs.com/product/features/gamified/
[120] V. Svabensky, P. Celeda, J. Vykopal, S. Brisakova, "Cybersecurity knowledge and skills taught in capture the flag challenges", Dec 2020, DOI 10.1016/j.cose.2020.102154
[121] ACM, IEEE, AIS SIGSEC, IFIP, "Joint Task Force on Cybersecurity Education. Cybersecurity Curricular Guideline;", Dec 2017, https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf
[122] Small Business Italia "Cos'e' la Gamification e come applicarla in azienda", October 2019, https://www.smallbusinessitalia.it/cose-la-gamification-e-come-applicarla-in-azienda/ (Italian)
[123] FreeDooMind, "Gamification in the company: games as a creative and non-competitive tool", September 2017, https://www.skilla.com/en/gamification-in-the-company-games-as-a-creative-and-non-competitive-tool/
[124] A. Hemmer, "LMS vs CMS vs LCMS What are the differences?", Mar 2021, https://www.easygenerator.com/en/blog/tools/differences-lms-cms/
[125] D.Bastanzhyieva, "eLearning Gamification: Its Role, Effectiveness, and Open edX Applications", Nov 2020, https://open.edx.org/blog/elearning-gamification-its-role-effectiveness-and-open-edx-applications/
[126] Moodle, "Plugins", https://moodle.org/plugins/?q=gamification
[127] D.Golubeva, "6 ideas for gamifying training with Kahoot! for businesses", June 2018, https://kahoot.com/blog/2018/06/20/gamification-tips-training-kahoot-businesses/
[128] GetPlayOff, "Your Agnostic Rules Engine", June 2018, https://www.getplayoff.com/features/
[129] Viewhooo, "Gamegagement Combine presentations and gamification. What you get is the next level of sharing information in a fun way.", https://viewhooo.com/
[130] Mambo, "Mambo Gamification Platform", 2021, https://mambo.io/gamification-platform
[131] Talentlms, "The LMS built for success", https://www.talentlms.com/
[132] Skillato, "Engagement and continuous e-learning for business performance", https://www.skillato.com/
[133] F.Viola, "Piattaforme di Gamification - Gametize", February 2020, https://www.gameifications.com/piattaforme-di-gamification-gametize/ (Italian)
[134] Gametize, "Create a gamified experience in just 5 minutes. Motivate and reward your audience with the world's simplest enterprise-grade gamification platform.", https://gametize.com/index
[135] Teaching and Language Lab, "Settimana della didattica", Feb 2022, https://www.politocomunica.polito.it/events/appuntamenti/settimana_della_didattica, (Italian)
[136] D. Pink, "The puzzle of motivation", TEDGlobal 2009, https://www.ted.com/talks/dan_pink_the_puzzle_of_motivation
[137] A. Nagarajan, J. M. Allbeck, A. Sood, T. L. Janssen, "Exploring game design for cybersecurity training", May 2012, DOI 10.1109/CYBER.2012.6392562
[138] Centrical, "Gamification Is There a One-size-fits-all Solution?", March 2016, https://centrical.com/gamification-is-there-a-one-size-fits-all-solution/
[139] Try Hack Me, "Advent of Cyber", 2021, https://tryhackme.com/christmas
[140] Politecnico di Torino, "Information Systems Security", 2020, https://didattica.polito.it/pls/portal30/gap.pkg_guide.viewGap?p_cod_ins=01TYMSM&p_a_acc=2021&p_header=S&p_lang=&multi=N
[141] Politecnico di Torino, "Cryptography", 2020, https://didattica.polito.it/pls/portal30/gap.pkg_guide.viewGap?p_cod_ins=03LPYOV&p_a_acc=2020&p_header=S&p_lang=IT&multi=N

[142] Politecnico di Torino, "Cybersecurity", 2020, https://didattica.polito.it/pls/portal30/gap.pkg_guide.viewGap?p_cod_ins=01UDROV&p_a_acc=2021&p_header=S&p_lang=IT&multi=N

[143] Politecnico di Torino, "Security Verification and Testing", 2020, https://didattica.polito.it/pls/portal30/gap.pkg_guide.viewGap?p_cod_ins=01TYAOV&p_a_acc=2021&p_header=S&p_lang=IT&multi=N

[144] M. Iorio, A. Palesandro, F. Risso, "CrownLabs - A Collaborative Environment to Deliver Remote Computing Laboratories", July 2020, DOI 10.1109/ACCESS.2020.3007961