POLYTECHNIC OF TURIN

Master of Science in Computer Engineering

Master Thesis

Security Serious Game

Advisors:
prof. Antonio Lioy
adj. prof. Andrea Atzeni

Candidate:
Manuel Sabelli

Academic Year 2021-2022

Summary

This thesis describes the problem of ignorance in CyberSecurity. This gap leads to Malware spreading. Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware uses human factors to spread, in fact, Malware authors often try to trick users into downloading malicious files or opening files containing malicious attachments. To avoid that, it is important to improve users' knowledge about Malware. One way to do that is through SSG. This is a technique for transmitting knowledge through gamification techniques, achieving good results.

The work starts talking about Cybercrime and how it is increased in the last few years. Then, it continues with the Malware description, how to protect from Malware and how Malware uses users' ignorance to spread. Regarding users' ignorance, there are some important statistics, before and after security training. They show how, where there was security training, employees were able to recognize malware in higher percentages.

Then, the work continues with Social Engineering and its different techniques: Baiting, Phishing, Pretexting, and Scareware.

After that, the work focuses on a way to reduce IT ignorance, in particular on Security Serious Games. The work starts to introduce the SSG and an important study about the target of the game. Because, before creating a game, you need to define a target. At the beginning of the study, there is Bartle's theory. He suggests a categorization of 4 types: Socializer, Achievers, Killers, and Explorers. This theory suffers from several limitations, then, another researcher Nick Yee formulated 3 components and 10 sub-components that are very important in understanding the motivations of the players.

After discussing the target, the work introduces a list of Serious Security Games online to better understand their mechanism. For each game, there is a short explanation about it, a personal review of the gameplay and then a way to adapt the game to the Malware concept. These SSGs are collected in a server, in which it is possible to read a short description to know the context of the game and it is possible to play it with a click on the play button.

Now, the work shifts to the creation of a SSG for teaching about Malware, in particular how it spreads.

In the end, the work, through the surveys, verifies if the users have acquired knowledge about Malware. Then, it discusses what has been achieved, what worked, and what can be better to improve in future works.

Acknowledgements

First of all, I would express my gratitude to Professor Lioy and Andrea Atzeni for allowing me to work on this interesting topic and for all their support.

I would like to thank all the experts who shared their knowledge about CyberSecurity and Security Serious Games, in particular.

I would also thank my family: my mother Nadia, my grandmother Carmela, my grandfather Nello and my uncles Fabio, Franco, and Luigi.

I thank my friends: Ale, Bett, Checco, Diego and Valerio, because they were always with me.

A special thanks to my father, I hope you are glad of me. I did my best to keep our promise.

Last but not least, I want to dedicate a line to myself for never giving up.

Contents

Chapter 1

Introduction

1.1 CyberCrime

Cybercrime is any criminal activity that involves a computer, networked device, or network. While most cyber crimes are carried out to generate profit for the cybercriminals, some cyber crimes are carried out against computers or devices directly to damage or disable them. Others use computers or networks to spread illegal information, images, or other materials. Instead, some cyber crimes do both (i.e., target computers to infect them with a computer virus, which is then spread to other machines and, sometimes, entire networks).

Cybercriminals may target an individual's private information or corporate data for theft and resale. As many workers settle into remote work routines due to the pandemic, cybercrimes are expected to grow in frequency in 2022, making it especially important to protect backup data. The Smart Working Observatory (2020) estimates that the number of workers involved could reach up to 5,350,000 (compared to 570,000 in 2019).

The necessity of internet connectivity has enabled an increase in the volume and pace of cybercrime activities because the criminal no longer needs to be physically present when committing a crime. The internet's speed, convenience, anonymity, and lack of borders make computer-based variations of financial crimes, such as ransomware, fraud, and money laundering, as well as crimes such as stalking and bullying, easier to carry out [1].

Cybercriminal activity may be carried out by individuals or groups with relatively little technical skill, or by highly organised global criminal groups that may include skilled developers with relevant expertise. To further reduce the chances of detection and prosecution, cybercriminals often choose to operate in countries with weak or non-existent cybercrime laws [2].

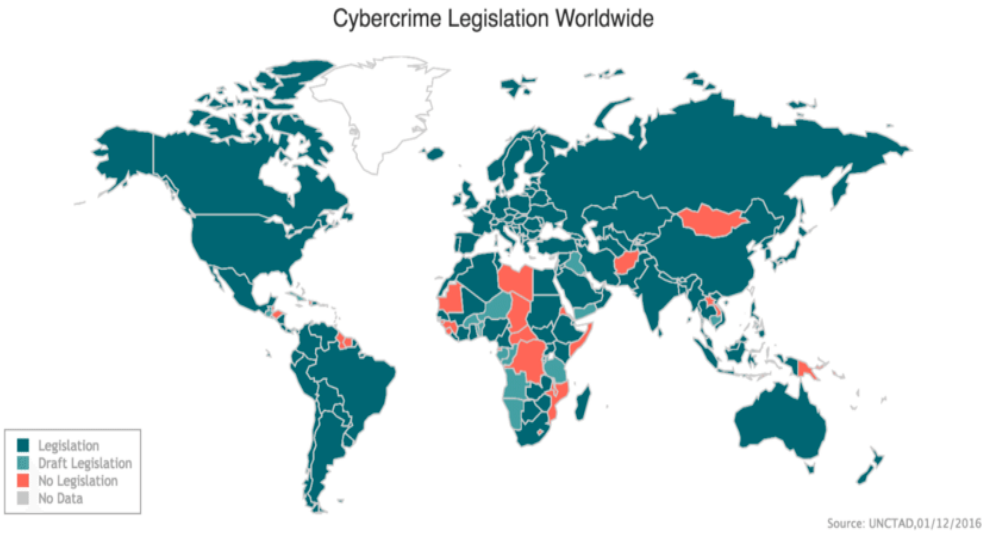

Figure 1.1. Cybercrime Legislation Worldwide (fonte: ResearchGate).

Cybercrime increasing in the last few years and it is becoming an important problem, following some statistics:

- In 2021, attacks around the world increased by 10% compared to the previous year. The new attack methods show that cybercriminals are increasingly sophisticated;
- The attacks classified by the researchers still occurred in 45% of cases in the American continent (slightly down compared to 2020). The attacks in Europe, on the other hand, increased (21%, against 16% the previous year), and in Asia (12%, compared to 10% in 2020). The situation of the attacks on Oceania (2%) and Africa (1%) remains substantially unchanged;
- The severity of attacks increased. In 2021, 79% of detected attacks had a "high" impact, compared to 50% last year. In detail, 32% were characterised by a "critical" severity and 47% as "high". Against these percentages, attacks with "medium" (-13%) and "low" (-17%) impact decreased;
- Ransomware attacks occur every 10 seconds;
- The global annual cost of cybercrime is estimated to be $ 10.5 trillion by 2025 [3].

1.2 Cybercrime affects on business

While the financial losses due to cybercrime can be significant, businesses can also suffer other disastrous consequences as a result of criminal cyberattacks, including the following: damage to investor perception after a security breach can cause a drop in the value of a company.

In addition to potential share price drops, businesses may also face increased costs for borrowing and greater difficulty in raising more capital as a result of a cyberattack. Loss of sensitive customer data can result in fines and penalties for companies that have failed to protect their customers' data. Businesses may also be sued over data breaches.

Damaged brand identity and loss of reputation after a cyberattack undermine customers' trust in a company and that company's ability to keep their financial data safe.

Following a cyberattack, firms not only lose current customers but also lose the ability to gain new customers. Businesses may also incur direct costs from a criminal cyberattack, including increased insurance premium costs and the cost of hiring cybersecurity companies to do incident response and remediation, as well as public relations and other services related to an attack [1].

1.3 What is Malware?

Cybercriminals attack in different ways to avoid detection and arrest. They often carry out their activities using Malware and other types of software.

Malware, short for "malicious software", refers to code developed by cyberattackers, designed to cause extensive damage to data and systems or to gain unauthorised access to a network [4].

Malware is a catch-all term used to define:

- Virus;
- Worms;
- Spyware;
- Trojans;
- Ransomware;
- Adware.

1.4 Why Malware?

The motives behind malware vary. In the past, many of these malware creators were pranksters trying to alleviate boredom and make a name for themselves.

While this is still true for some, most people who create malware do so for purely criminal purposes such as:

- tricking a victim into providing personal data for identity theft;
- stealing consumer credit card data or other financial data;
- assuming control of multiple computers to launch denial-of-service attacks against other networks;
- infecting computers and using them to mine bitcoin or other cryptocurrencies.

Although malware cannot damage the physical hardware of systems or network equipment, it can steal, encrypt, or delete your data, alter or hijack core computer functions, and spy on your computer activity without your knowledge or permission.

1.5 How to protect from Malware?

With cyber threats on the rise and Malware occurrences becoming increasingly common, there is no better time than now to implement a robust cybersecurity defense against Malware. The best way to do this is by:

- avoid clicking on pop-up ads while browsing the Internet;
- avoid opening email attachments from unknown senders;
- keeping comprehensive, easily recoverable backups;
- do not click on strange, unverified links in emails, texts, and social media messages;
- scan your downloads.

1.6 How does Malware spread?

Malware can spread in any number of ways: by email, they may have infected attachments; by direct vectors including using a USB infected device; by websites designed by cyber criminals that exploit system vulnerabilities. Another way is through users, who can be prone to temptation ("check out this cool website!") or easily led by other emotions such as fear ("install this antivirus software immediately").

"Malware attacks would not work without the most important ingredient: you [5]."

Education is key to ensuring users are aware of the risk of malware and what they can do to prevent an attack.

The types of vulnerabilities that have the greatest negative impact on corporate security concern the lack of awareness of employees concerning the policies and good practices of conduct introduced in the company, the distraction of users, mobile access to corporate information, and the increasingly widespread presence of personal mobile devices, often also used for work purposes.

In fact, alongside the technological vulnerabilities, due for example to the backwardness of the IT architecture or the failure to update systems, which can be targeted by hackers to pursue their malicious purposes, it is estimated that a large percentage of cyber-attacks are caused by human behavior. Employees often act naively or unwittingly, making it easier for cybercriminals to bypass the security measures put in place by the company.

A report published found that of 1,000 public sector staff, nearly half had never even heard of ransomware, let alone two-factor authentication. Yet the research today from a data security provider, Reading-based Clearswift, emphasizes alarmingly low levels of cybersecurity awareness that are compounded by a lack of training. (Some 32 % said they are trained once a year or less often; 16 % never get cybersecurity training). With one UK council (Redcar) estimating the repair bill from a ransomware attack in February at between 11 million dollars and 18 million dollars, the case for security investment, including basic training, is a no-brainer.

1.7 IT ignorance statistics

Less than a quarter of people aged between 23 and 38 (so-called millennials) can correctly define the term "ransomware", more than one-fifth of British people don't know how to change their Wi-Fi security settings, and one-third of Australian ones "don't feel the need" to ever use a VPN, 30% of Americans think "malware" is something used to extend the range of a Wi-Fi router, and 50% of people who take a work device home have let their friends and family use it.

These were just some of the more intriguing findings, which highlighted the scale of ignorance among end-users when it comes to cyber security, the scale of the challenge facing security professionals, and the scale of the security industry's failure to educate.

In a world where 90% of global organizations surveyed said they had been targeted by business email compromise (BEC) and spear phishing attacks, there are data from nearly 50 million simulated phishing attacks, third-party survey responses by security professionals in Australia, France, Germany, Japan, Spain, the UK and the US, and 3,500 working adults.

We found that the majority of people, in general, failed to observe the basic principles of cyber security hygiene. For example, 45% admitted to password reuse, more than 50% did not password protect their home networks, 32% were unfamiliar with VPNs, and 90% used their work PCs and smartphones for personal activities.

Recognition of common security terms, such as malware, phishing, and ransomware, was also found to be lacking. Only 61% could correctly define phishing, and only 31% malware, exposing both a knowledge gap and a language barrier for security educators. Recognition also varied wildly between age groups. Millennials tended to underperform in security awareness, reflecting other recent studies on the same topic, although it is not clear why this should be. This makes

that 85% of cybersecurity breaches are caused by human error and 94% of all malware is delivered via email.

"Effective security awareness training must focus on the issues and behaviors that matter most to an organization's mission," said Joe Ferrara, senior vice-president, and general manager of security awareness training at Proofpoint (an American enterprise security company).

"We recommend taking a people-centric approach to cyber security by blending organization-wide awareness training initiatives with targeted, threat-driven education. The goal is to empower users to recognize and report attacks [6]."

1.8 Statistics after security training

Where appropriate security awareness training was undertaken, the effects were noticeable, with 78% of surveyed organisations saying they had seen "measurable reductions" in phishing susceptibility as a result.

Growth in end-user email reporting, which is a key metric when it comes to understanding and gauging positive behaviours, was another positive trend picked out by the report. More than nine million suspicious emails were reported in 2019, up 67% from 2018. It is a good sign because it suggested end-users were becoming more vigilant and better able to identify threats, a useful skill given the noted trend towards more targeted and personalised forms of attack.

Altogether, 5% of the organisations surveyed said they had dealt with one successful phishing attack last year, and security pros reported high volumes of social engineering attempts. A total of 88% said they had seen spear-phishing attempts, 86% reported BEC attacks, 84% SMS/text phishing or smishing, 83% voice phishing or vishing, and 81% malicious USB drops.

A clear majority of organisations also reported that they were now taking corrective action against users who make repeated mistakes related to phishing attacks, with many respondents saying employee awareness improved vastly if people were made to bear the consequences. The UK was the country most likely to impose some monetary penalty on repeated victims, while organisations in France were most likely to fire them.

Some reports also showed that 65% of surveyed professionals reported that their organisation had experienced a ransomware infection in 2019. Of these, 33% opted to pay up against all advice, while 32% held firm. Of those that negotiated, 9% found they were extorted for further payments, and 22% never got access to their data [6].

1.9 Social Engineering

The advancements in digital communication technology have made communication between humans more accessible and instant. However, personal and sensitive information may be available online through social networks and online services that lack the security measures to protect this information. Communication systems are vulnerable and can easily be penetrated by malicious users through social engineering attacks. These attacks aim at tricking individuals or enterprises into accomplishing actions that benefit attackers or providing them with sensitive data such as social security numbers, health records, and passwords.

Scams based on social engineering are built around how people think and act. As such, social engineering attacks are especially useful for manipulating user behavior. Once an attacker understands what motivates a user's actions, they can deceive and manipulate the user effectively.

In addition, hackers try to exploit a user's lack of knowledge. Users may not realize the full value of personal data, like their phone numbers. As a result, many users are unsure how to best protect themselves and their information.

What makes social engineering especially dangerous is that it relies on human error, rather than vulnerabilities in software and operating systems. Humans are more likely to trust other

humans compared to computers or technologies and mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion. Social engineering is one of the biggest challenges facing network security because it exploits the natural human tendency to trust.

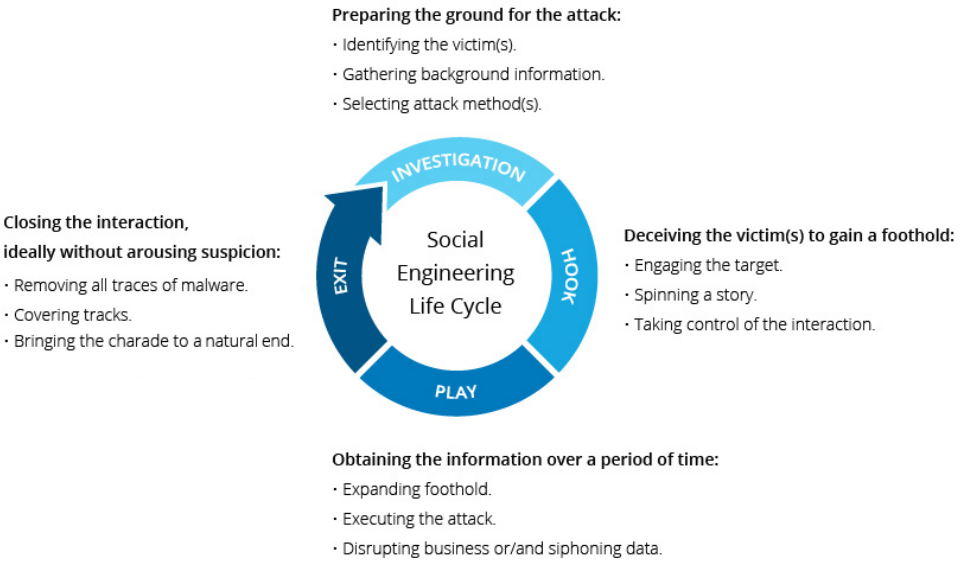

Figure 1.2. Social Engineering attack schema (fonte: Imperva).

Although social engineering attacks differ from each other, they have a common pattern with similar phases. The common pattern involves four phases: (1) collect information about the target; (2) develop a relationship with the target; (3) exploit the available information and execute the attack; and (4) exit with no traces. Figure 1.2 illustrates the different stages of a social engineering attack [7].

1.10 Social Engineering Techniques

Social engineering attacks come in many different forms and can be performed anywhere where human interaction is involved. The following are the five most common forms of digital social engineering assaults.

1.10.1 Baiting

As its name implies, baiting attacks use a false promise to pique a victim's greed or curiosity. They lure users into a trap that steals their personal information or inflicts their systems with malware. The most reviled form of baiting uses physical media to disperse malware. For example, attackers leave the bait, typically malware, infected flash drives-in conspicuous areas where potential victims are certain to see them (e.g., bathrooms, elevators, the parking lot of a targeted company). The bait has an authentic look to it, such as a label presenting it as the company's payroll list. Victims pick up the bait out of curiosity and insert it into a work or home computer, resulting in automatic malware installation on the system. Baiting scams don't necessarily have to be carried out in the physical world. Online forms of baiting consist of enticing ads that lead to malicious sites or that encourage users to download a malware-infected application.

1.10.2 Scareware

Scareware involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit (other than for the perpetrator) or is malware itself. Scareware is also referred to as deception software, rogue scanner software, and fraudware. A common scareware example is the legitimate-looking pop-up banners appearing in your browser while surfing the web, displaying text such as, "Your computer may be infected with harmful spyware programs." It either offers to install the tool (often malware-infected) for you, or will direct you to a malicious site where your computer becomes infected. Scareware is also distributed via spam email that doles out bogus warnings or makes offers for users to buy worthless/harmful services.

1.10.3 Pretexting

Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim to perform a critical task. The attacker usually starts by establishing trust with their victim by impersonating co-workers, police, bank and tax officials, or other persons who have right-to-know authority. The pretexter asks questions that are ostensibly required to confirm the victim's identity, through which they gather important personal data. All sorts of pertinent information and records are gathered using this scam, such as social security numbers, personal addresses, phone numbers, phone records, staff vacation dates, bank records, and even security information related to a physical plant.

1.10.4 Phishing

As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity, or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware. An example is an email sent to users of an online service that alerts them of a policy violation requiring immediate action on their part, such as a required password change. It includes a link to an illegitimate website, nearly identical in appearance to its legitimate version, prompting the unsuspecting user to enter their current credentials and new password. Upon form submittal, the information is sent to the attacker. Given that identical, or near-identical, messages are sent to all users in phishing campaigns, detecting and blocking them is much easier for mail servers having access to threat-sharing platforms.

1.10.5 Spear phishing

This is a more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises. They then tailor their messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less conspicuous. Spear phishing requires much more effort on behalf of the perpetrator and may take weeks and months to pull off. They're much harder to detect and have better success rates if done skillfully.

1.11 Security Dissemination

The digital era of today is marked by the proliferation of software systems across various platforms used in our daily lives. Examples include mobile phones, laptops, smart watches, etc. It is of utmost importance that the systems continuously provide us with their intended services. The importance of security and privacy protection of these systems has drastically increased due to their penetration in every walk of life, e.g., business, hospitals, education, etc. Software security emphasizes the matter which makes software work correctly even under malicious attacks. Attaining and sustaining security levels impose complex and interdisciplinary challenges. To make

software systems work as they are intended, the training, awareness, and education of the end users regarding system security are of great importance.

Protecting people from cyber threats imposes great challenges, not only technically, but also socially. To achieve the intended level of awareness, software security principles need to be shown with concrete examples during security education. Many technical security protection measures have been developed and deployed in today's information systems. However, security protection still requires a holistic understanding of human psychology and behavior. Since they are one of the most vulnerable targets in the loop. Thus, enhancing the security knowledge of the system actors and improving their security awareness is of great importance. Among the many methods being developed and used to conduct security training, game-based approaches are considered potentially one of the most useful and effective ones [8].

Chapter 2

Background

2.1 Game-based Learning

Game-based learning and Serious Game can become very useful methods at school and in learning, especially now that digital education has assumed a fundamental role in guaranteeing the right to study pupils in this period of quarantine caused by the coronavirus emergency.

Game-Based Learning means learning achieved through the use of games or video games, which can sometimes be born as entertainment tools but which are then used, with or without modifications, to achieve an educational goal.

The word "empathy" is perhaps the key to everything. The game, and in particular digital games, unlike other mediums, allow you to immerse yourself in scenarios and settings that are difficult to represent in reality, and in doing so you can put yourself "in the shoes of others", to be the protagonists in first person [9].

2.2 Security Serious Game: What it is?

When games and video games are applied to non-playful contexts we speak of "serious games". Introducing serious games in teaching certainly means radically changing the teaching methodology, it means including a new language, learning based on game levels, group activities, on the achievement of objectives through scores and prizes.

These immersive technologies allow children and young people not only to develop empathy but also to learn by doing, stimulating and encouraging creativity, concentration, collaboration, learning by trial and error, memory, exploration, and critical interaction through language and media.

Given the complexity of some IT security topics, the main purpose is to show how cyber attacks work in a more accessible, exemplified and interactive way than a textual explanation of the topic.

2.3 Gamification: What it is?

Gamification means the application of game mechanics and dynamics to non-game situations to foster the active interest of users and their involvement, in encouraging the performance of an activity or the acquisition of behavior. It, therefore, acts at the level of the player's motivation through the adoption of some game mechanics such as game levels, challenges, rewards, and points.

Dividing a process into levels helps to define individual goals and increase motivation, the assignment of rewards allows students, for example, to receive immediate feedback on their performance, while the scoring mechanism and player ranking stimulate healthy competition. The principle behind gamification is very simple: if we have fun, we get better results.

2.4 Security Serious Game: Target

Before creating a Serious Game, you need to define a target. The target is the portion of the public to the serious game will address. Usually, we are aimed at an audience that already has basic knowledge in the IT field, but at the same time has not knowledge about IT security subject. This allows to show concepts with a greater level of detail.

Knowing who plays or will play in our system, and the reasons that push it is a fundamental preparatory action that helps to identify the best Gamification techniques to meet certain needs rather than others. It is impossible to create a design for a universal audience, establishing one or more target audiences is essential for ultimate success.

2.4.1 Bartle's Player Types

Bartle's Player Types are a well-known model of player motivations. The types identified by Bartle refer mainly to the MMORPG context, but at the same time provide an excellent base from which to create gamified experiences, given that they refer to the playful environment in general. In addition, they are used in numerous gamification-related frameworks. Bartle provides important insight into how players may differ from one another and he suggests a categorization of 4 Types (Socializer, Achievers, Killers, and Explorers) based on two underlying axes.

Figure 2.1. Bartle's Player Types (fonte: ResearchGate).

Dr. Bartle created a series of A/B answer questions, to determine which type a player tended to lean toward. The Bartle Test of Gamer Psychology was subsequently converted into digital forms and can be seen right here (see Figure 2.2/2.3/2.4) [10].

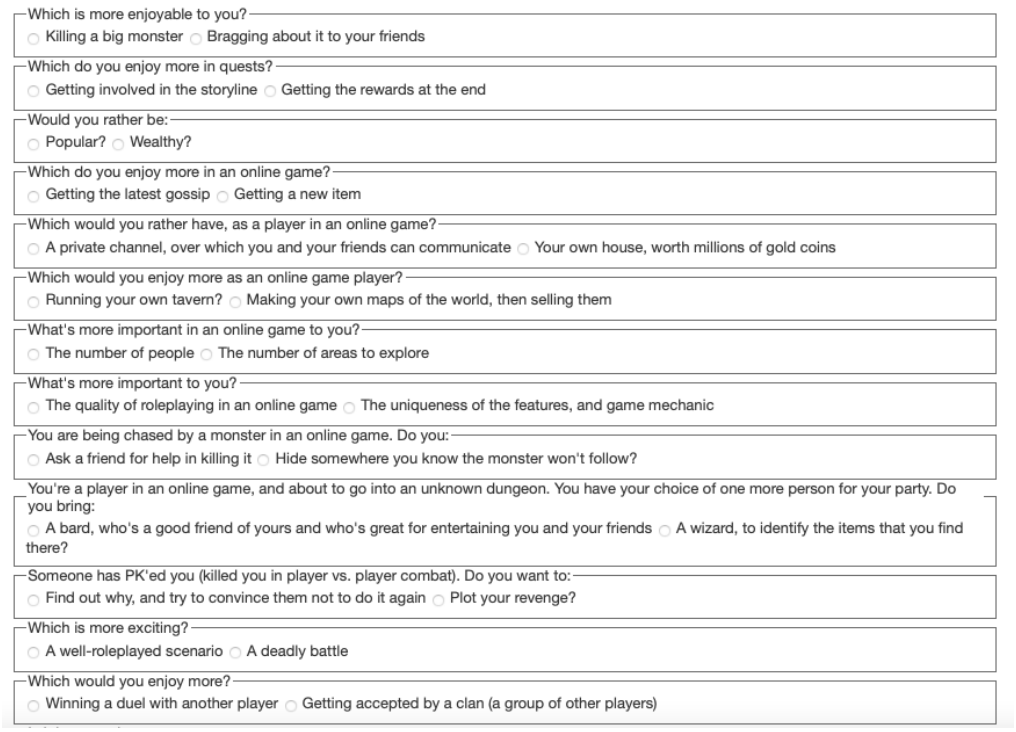

Figure 2.2. The Bartle Test of Gamer Psychology pt.1.

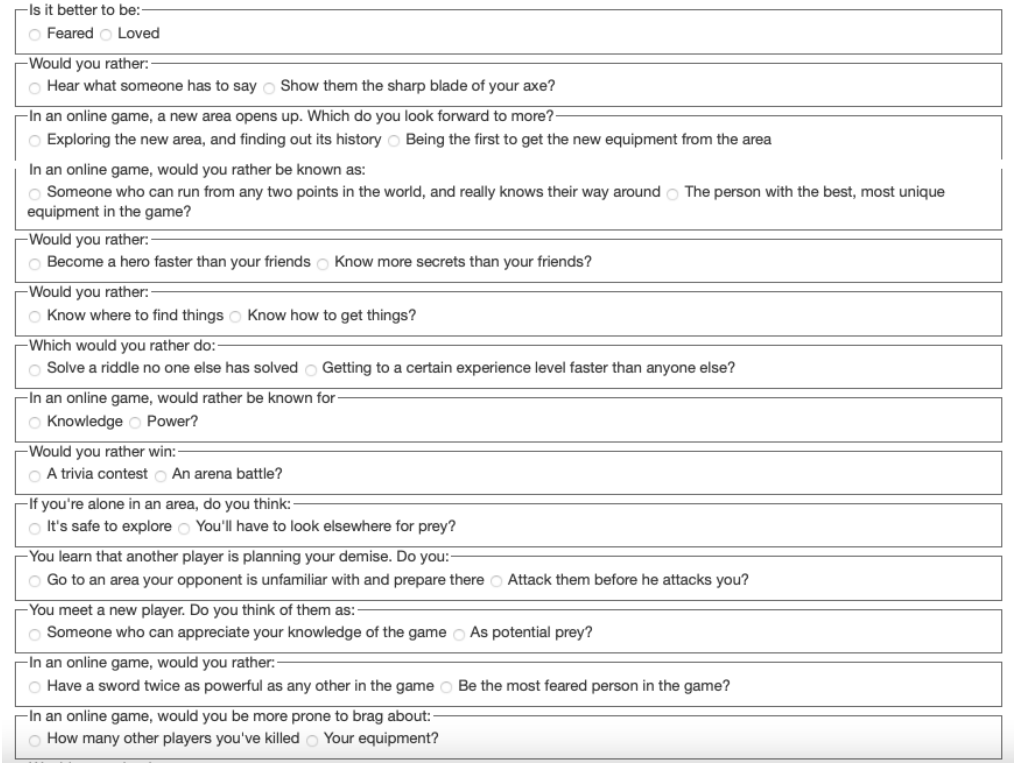

Figure 2.3. The Bartle Test of Gamer Psychology pt.2.

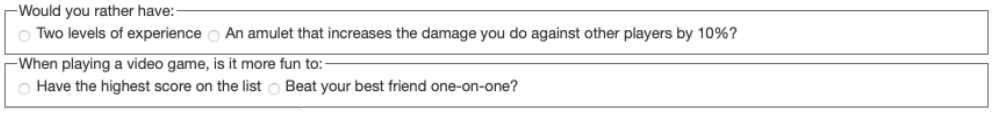

Figure 2.4. The Bartle Test of Gamer Psychology pt.3.

Although all personality tests require a degree of scepticism (due to what someone says they would do in a particular scenario compared to what they would do, not quite lining up), Bartle's system is a useful shorthand way of describing players.

Bartle's theoretical model, while providing important insight, suffers from several limitations.

- 1) Proposed components of each Type may not be related. For example, Bartle proposes that role-playing and socialization both fall under the same Type, but they may not be highly correlated.
- 2) Proposed Types may overlap with each other. For example, aren't members of raid-oriented guilds both Achievers and Socializers? But in Bartle's Types, they are on opposite corners of the model.
- 3) The purely theoretical model provides no means to assess players as to what type they are. But more importantly, without resolving the problem in (1), any attempted assessment of players based on this model might be creating player types rather than measuring them.

2.4.2 The Daedalus Project

Nick Yee is an American researcher, proponent of the Daedalus project on the sociology and psychology of MMORPGs (massively multiplayer online role-playing games) in which he collected data from over 40,000 players [11].

Yee was highly critical of Bartle's taxonomy of players, particularly of Bartle's assumptions that a preference for one type of play suppressed others and the fact that Bartle never empirically tested whether this was indeed the case.

His studies are closely connected with Bartle's research, taking a step further, however, giving the quantitative contribution that was previously lacking, proposing an empirical model.

His main interest was to understand how videogame players differ and what their motivations for playing are also about gender, age, and gaming behaviors.

Therefore, starting from Bartle's qualitative research, Yee formulated 3 components and 10 sub-components that are important in understanding the motivations of the players.

The Achievement Component:

Advancement: Gamers who score high on this subcomponent derive satisfaction from reaching goals, leveling quickly and accumulating in-game resources such as gold. They enjoy making constant progress and gaining power in the forms offered by the game - combat prowess, social recognition, or financial/industrial superiority. Gamers who score high on this subcomponent are typically drawn to serious, hard-core guilds that can facilitate their advancement.

Mechanics: Gamers who score high on Mechanics derive satisfaction from analyzing and understanding the underlying numerical mechanics of the system. For example, they may be interested in calculating the precise damage difference between dual-wielding one-handed swords vs. using a two-handed sword, or figuring out the resolution order of dodges, misses, and evasions. Their goal in understanding the underlying system is typically to facilitate templating or optimizing a character that excels in a particular domain.

Competition: Gamers who score high on this subcomponent enjoy the rush and experience of competing with other gamers on the battlefield or economy. This includes both fair, constrained

Achievement	Social	Immersion
Advancement Progress, Power, Accumulation, Status	**Socializing** Casual Chat, Helping Others, Making Friends	**Discovery** Exploration, Lore, Finding Hidden Things
Mechanics Numbers, Optimization, Templating, Analysis	**Relationship** Personal, Self-Disclosure, Find and Give Support	**Role-Playing** Story Line, Character History, Roles, Fantasy
Competition Challenging Others, Provocation, Domination	**Teamwork** Collaboration, Groups, Group Achievements	**Customization** Appearances, Accessories, Style, Color Schemes
		Escapism Relax, Escape from RL, Avoid RL Problems

Figure 2.5. 3 main components and their subcomponents. (fonte: Daedalus).

challenges - such as dueling or structured PvP/RvR, as well as unprovoked acts - such as scamming or griefing. Gamers who score high on this subcomponent enjoy the power of beating or dominating other players.

The Social Component:

Socializing: Gamers who score high on this subcomponent enjoy meeting and getting to know other gamers. They like to chit-chat and gossip with other players as well as helping out others in general - whether these be less-experienced players or existing friends. Gamers who score high on this subcomponent are typically drawn to casual, friendly guilds.

Relationship: Gamers who score high on this subcomponent are looking to form sustained, meaningful relationships with others. They do not mind having personal and meaningful conversations with others that touch on RL issues or problems. They typically seek out close online friends when they need support and give support when others are dealing with RL crises or problems.

Teamwork: Gamers who score high on Teamwork enjoy working and collaborating with others. They would rather group than solo, and derive more satisfaction from group achievements than from individual achievements. Gamers who score low on this subcomponent prefer to solo and find it extremely important to be self-sufficient and not have to rely on other gamers. They typically group only when it is absolutely necessary.

The Immersion Component:

Discovery: Players who score high on Discovery enjoy exploring the world and discovering locations, quests or artifacts that others may not know about. They enjoy traveling just to see different parts of the world as well as investigating physical locations (such as dungeons and caves). They enjoy collecting information, artifacts or trinkets that few others have.

Role-Playing: Players who score high on Role-Playing enjoy being immersed in a story through the eyes of a character that they designed. These players typically take time to read or understand the back-story of the world as well as taking time to create a history and story for their characters. Also, they enjoy role-playing their characters as a way of integrating their character into the larger ongoing story of the world.

Customization: Players who score high on this subcomponent enjoy customizing the appearance of their characters. It is very important to them that their character has a unique style or appearance. They like it when games offer a breadth of customization options and take time to make sure that their character has a coherent color scheme and style.

Escapism: Gamers who score high on Escapism use the environment as a place to relax or relieve their stress from the real world. These players may use the game as a way to avoid thinking about their RL problems or in general as a way to escape RL.

2.5 Security Serious Game Online

In this phase of the work, I did testing and revision of various Security Serious Games present online [12]. This work aims to understand the dynamics behind the various SSGs, to develop one that is logically correct, playable, has a well-defined purpose, and above all useful to the target that will use it.

2.5.1 CryptoClub

Web Site: https://www.cryptoclub.org/

On this site there are several sections containing very simple mini-games for players in the world of removal.

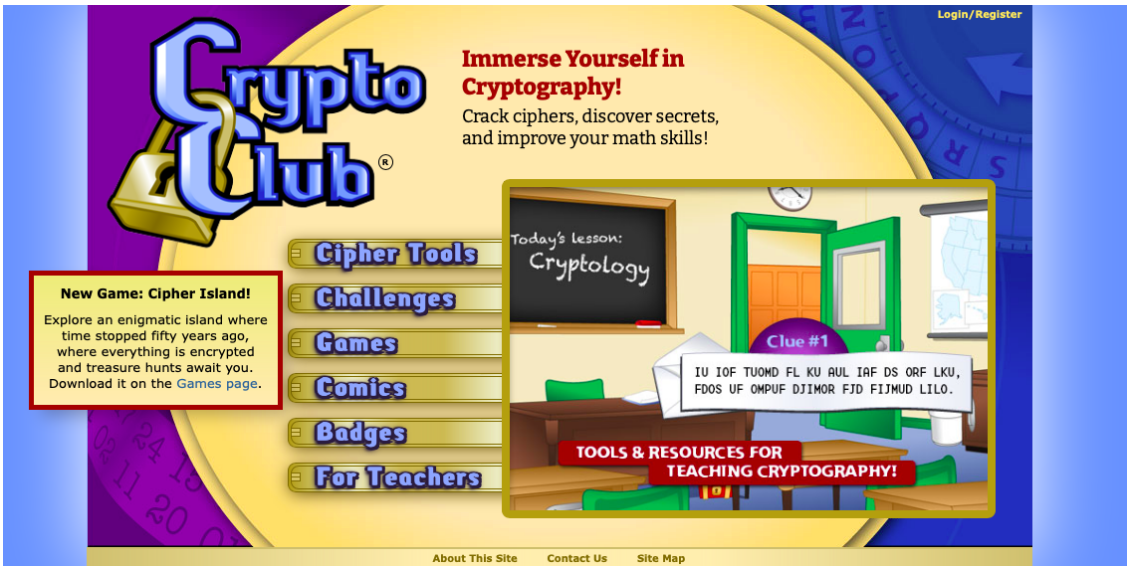

Figure 2.6. Crypto Club start menu.

Most games don't need installation so you can play them directly online. At first, perhaps it is not so easy to understand the mechanism, it would take more precise indications of what must be done. After a few minutes of play, however, you will know how it works then playing is easier.

The Cipher Tools section shows the practical operation of simple substitution encryption algorithms (including Caesar cipher and Vigenere cipher), both in the act of encrypting and decrypting a message. There are also a couple of cracking tools based mostly on exploiting the frequency of letters in the English language.

Figure 2.7. Crypto Club Cipher Tools.

There is also a section reserved for comics which contains a couple of comics dealing with the subject of cryptography. Knowledge about cryptography is conveyed through storytelling with simple themes: such as encrypting a message that reveals the whereabouts of a buried treasure, or using encrypted communication to conspire against Queen Elizabeth I.

Figure 2.8. Crypto Club Comics.

CryptoClub is very interesting if you want to learn technical skills about cryptography but it's not ideal for malware knowledge. Maybe could be introduced new mini-games with concepts about Malware: for example a new section "Malware" with a mini-game regarding phishing email, virus, DoS, etc. And at the end, also the game can be integrated with a survey so the user can see his progress.

2.5.2 Cyberciege

Web Site: https://nps.edu/web/c3o/downloads

There are many levels of play where the main topics of cyber security are covered. The gameplay is that of a management game in which the player has available resources (game currency) and must decide how to invest them to efficiently and effectively protect assets from cyber attacks, with the possibility of implementing a great variety of countermeasures.

2.5.3 BigBro

Web Site: https://bitbucket.org/BlackDavid/securityseriousgame

It is a quiz game, in which the player must correctly answer different types of questions. The topics covered are:

- a general introduction to IT security concepts such as authentication, integrity, etc.
- a theoretical introduction to the various types of cyber attacks;
- best known symmetric encryption algorithms;
- some brief notes on digital signatures.

2.5.4 CyberCraft

Web Site: https://github.com/luyangshang/CyberCraft

Figure 2.9. CyberCraft Start Menu.

Due to its structure, based mainly on playability and not on teaching, the game can be aimed at a fairly heterogeneous audience of users. The game is not very involved, and it is very mechanical. While using it, you don't understand exactly what you are doing. For example, it is not clear how the resources used for learning defense techniques are recharged. Or when defense techniques are sufficient to stop an attack or not. The aim of the game is to introduce some cybersecurity concepts by emphasizing the attack-countermeasure relationship of the techniques described. Even in this, however, while you play you do not acquire notions, but countermeasures are just applied.

Figure 2.10. Personal Notes (Theory Section).

By clicking on the notes at the top left, instead, there is the theory section. One solution to improve gameplay and understanding could be to integrate more theory into the game instead of keeping the two parts completely separate. In this way, the user can learn directly by playing the game.

2.5.5 SimScada

Web Site: https://github.com/serranda/SecuritySeriousGame

The gameplay is that of a management / tycoon game, in which the player must manage the security of a company that works with SCADA systems. You have to decide how to invest the funds at your disposal while keeping your balance sheet in surplus. We need to react to the unexpected, that is, the attacks that hit the company, and learn how to prevent possible risks (even by following suggestions) before they can materialize into attacks and cause damage. In game it is possible to consult an encyclopedia in which some lessons are available on the topics covered. There are no in-depth technical aspects in the game mechanics, but rather the cause-effect-countermeasure relationships between security threats, attacks suffered and defense systems are established.

2.5.6 Centigrade

Web Site: https://cybersecurity.centigrade.de/

The games is composed by 3 different minigames.

- Documents, please;
- Spam Defense;
- Hack the Planet.

All three games are easy and useful for understanding CyberSecurity concepts. The graphics help in understanding what needs to be done during the game. As for the first game (Documents, please), documents are shown and you need to understand, through the confidentiality levels (see Figure 2.11) where they should be placed: normal email, encrypted email, trash, paper shredder, social, or cloud (see Figure 2.12).

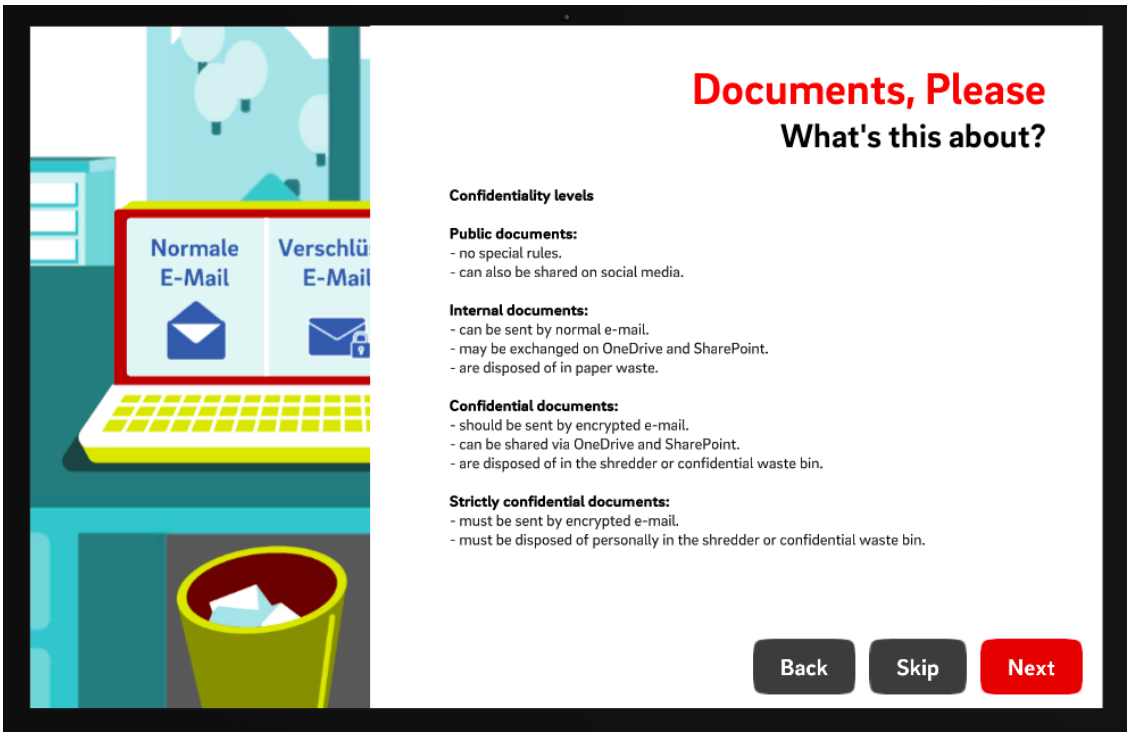

Figure 2.11. Confidentiality levels.

Figure 2.12.

At the end of the game, a report (see Figure 2.13) with the user's score based on correct and wrong answers is shown. This is a good technique to see if there are any improvements and to understand the user's initial level of computer knowledge.

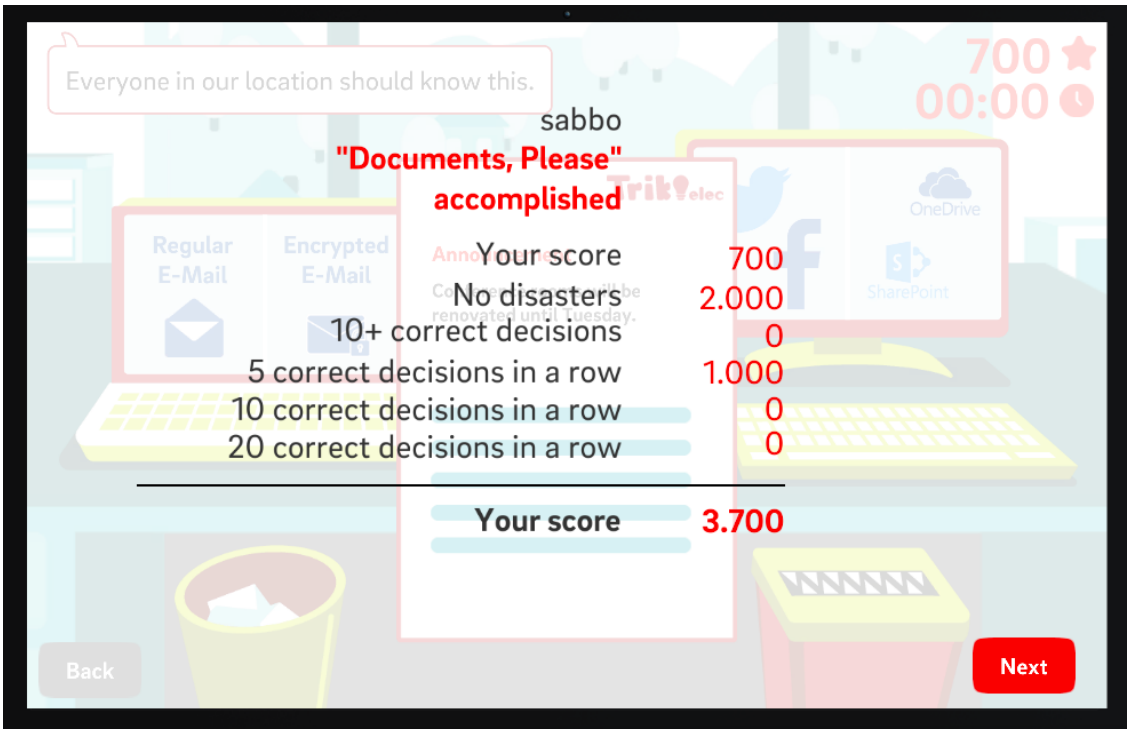

Figure 2.13. User Report

The second game (Spam Defense), on the other hand, is divided into two parts. A part where the user takes the role of the attacker (see Figure 2.14): in this case, data about the victim are provided in the left side of the window (for example a side of his character, or a passion for it, etc.) and through those data, emails of three blocks must be composed to attract the victim. This is how phishing is done by the attacker.

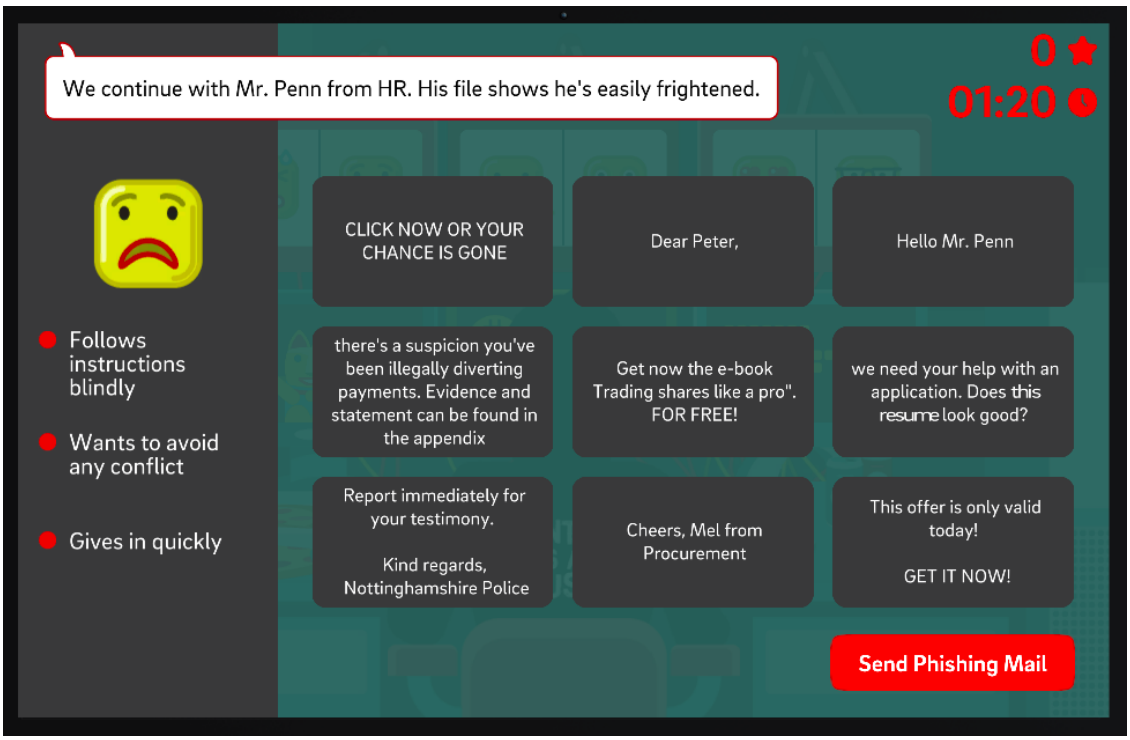

Figure 2.14. Spam Defense, Attacker Side

In the second part of the game, however, the user personifies himself in the role of the victim. You will receive emails, and you need to understand which of these is a “Regula E-mail”, “Phishing” or “Spam” (see Figure 2.15). This is linked to the main theme of the thesis and is a good technique to make a user understand if it is Malware, in this case, phishing emails, or not.

Like in the first game, also in here it is present a report with the right and wrong answers.

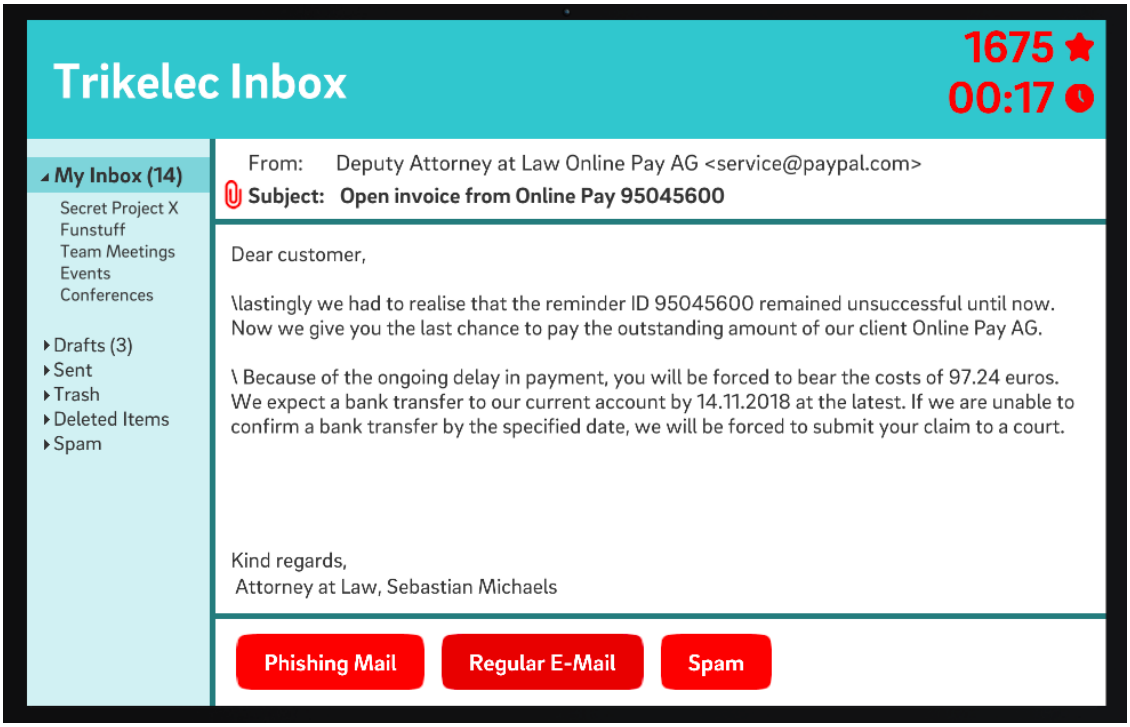

Figure 2.15. Phishing Email Example

In the last game, instead, through the information present in the users' social profiles (see Figure 2.16), an attempt is made to carry out a brute force attack to find the access passwords. Also, this game is easy to understand and allows you to assimilate the basic concepts behind this hacking technique.

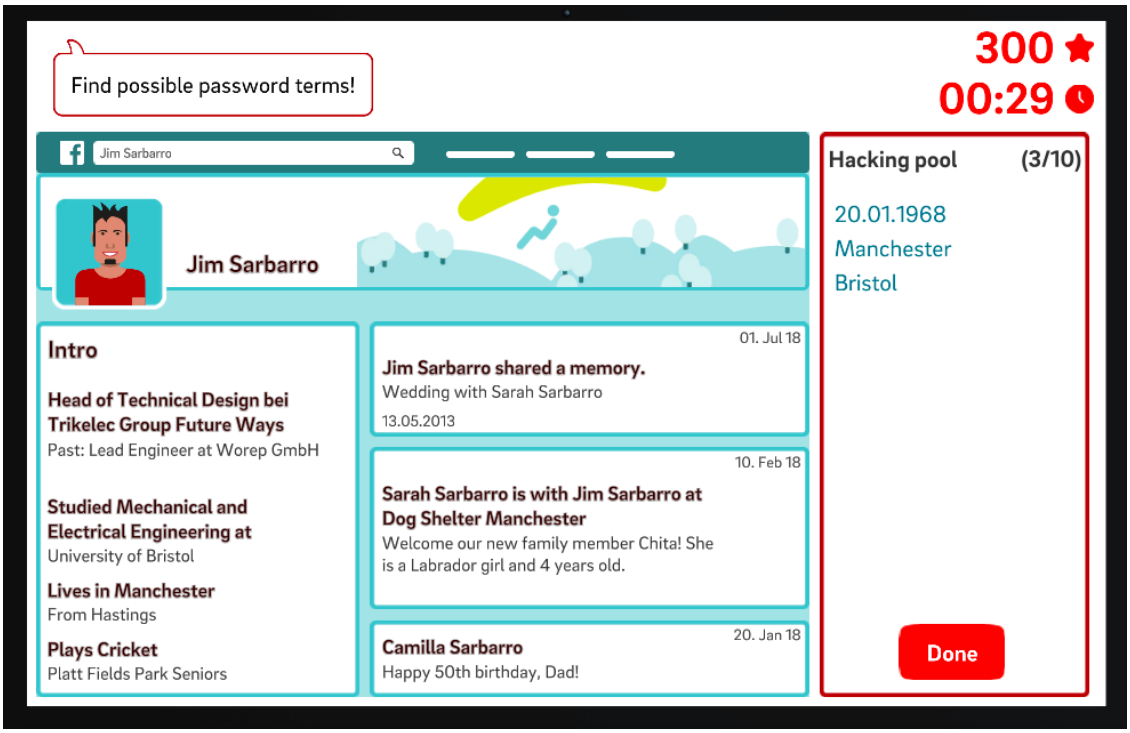

Figure 2.16. Social Profile with user's informations

At the end you will have the report of the attack, in here you can see which words were useful to compute the attack, how long the attack takes to find the password and the found password (see Figure 2.17).

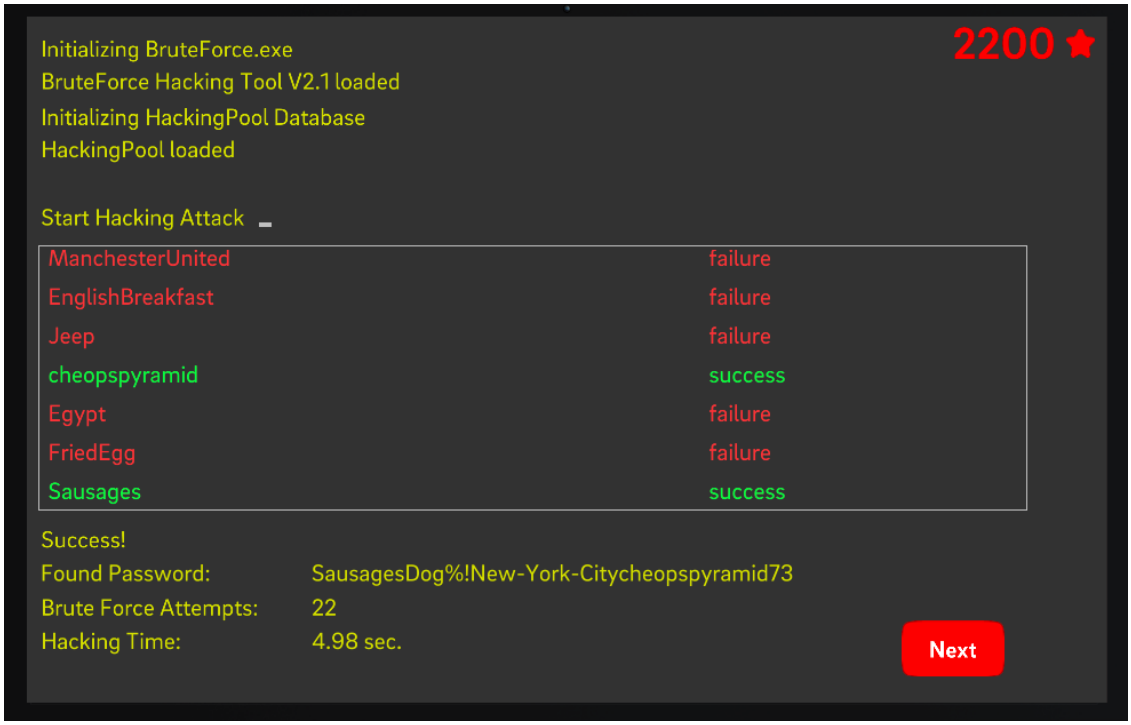

Figure 2.17. Brute Force Attack Report

2.5.7 DropIT!

Web Site: https://bitbucket.org/alexander_doni/dropit-a-personal-firewall-security-serious-game

It is a quiz game to which a platform style has been applied. Before each level, the player is presented with the topics covered and is instructed on the possible threats that will arise. The player holds the role of newly hired IT security officer of the company. The environment in which he operates is a room in which there are 6 doors (3 incoming and 3 outgoings) and 4 mainframes, which represent the company's assets.

The goal is to make users aware of the cyber security threats that need to be faced in everyday life, also providing an introduction to the use of personal firewalls.

2.5.8 Insector

Web Site: https://github.com/davidpereza7/InSecTorv1

The game consists of a series of multiple choice quizzes with one or more correct answer options. The questions deal with basic IT security issues, which mainly focus on attacks and related countermeasures to be adopted.

2.5.9 Minigiochi a tema Security

Web Site: http://gost.iitd.ac.in/serious_games/pages/ser.html

- Phishing: This game aims to expose players to phishing attacks to show them how they can protect their data from threats;

  In this first part, the user will face everyday work situations such as the receipt of a voice mail (see Figure 2.18), or the arrival of an email (see Figure 2.19). The user is then tested and, in the case of voice mail, a choice must be taken whether the data can be provided or whether it is a malicious voice mail. In the case of an email, on the other hand, the user must recognize based on the data provided: sender and text of the email, if that can be a regular email or a phishing email.

Figure 2.18. Voice Mail

- Authentication: This game wants to encourage users to use more complex passwords, avoiding low-security ones;

  The game has been set up in a way where you need to grab all the passwords matching certain criteria and avoiding others.

- Firewall: This game aims to teach the player some concepts regarding firewalls, also using basic concepts related to networks (see Figure 2.21).

- Blockchain: this game wants to introduce some basic knowledge regarding how blockchains work (see Figure 2.22);

- Threat identification: the aim is to teach to identify the threats that the player finds himself identifying;

- ARP spoofing: aims to show how the attack of the same name works.

Below is a group of games that have the same structure, but deal with different vulnerabilities. The topics covered are:

- Components with known vulnerabilities;

- Cross-Site Scripting (XSS): in this game, the XSS attack is explained through a simile (see Figure 2.23). Once the user has learned what an XSS attack is, he is shown a website (see Figure 2.24) and has to find the elements that can be used for this attack.

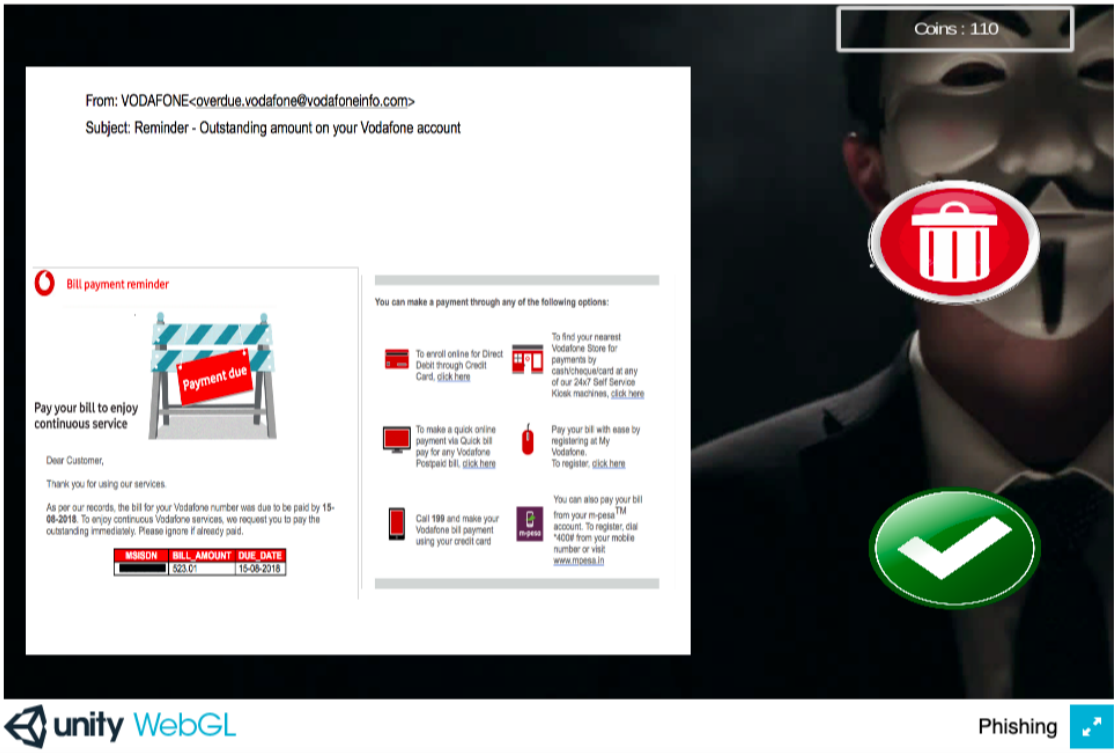

Figure 2.19. Email

Figure 2.20. Hints for a strong Password.

- Insufficient logging and monitoring: there are quizzes which are useful to learn logging and monitorin concepts (see Figure 2.25).

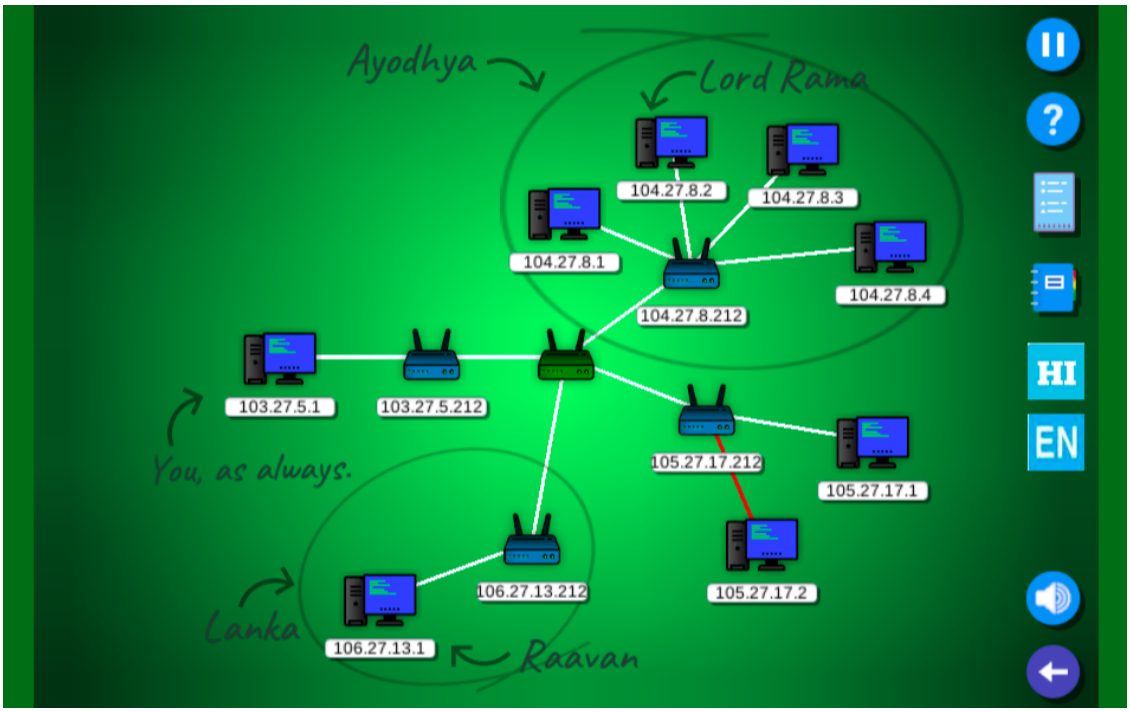

Figure 2.21. Network composed by hosts and routers.

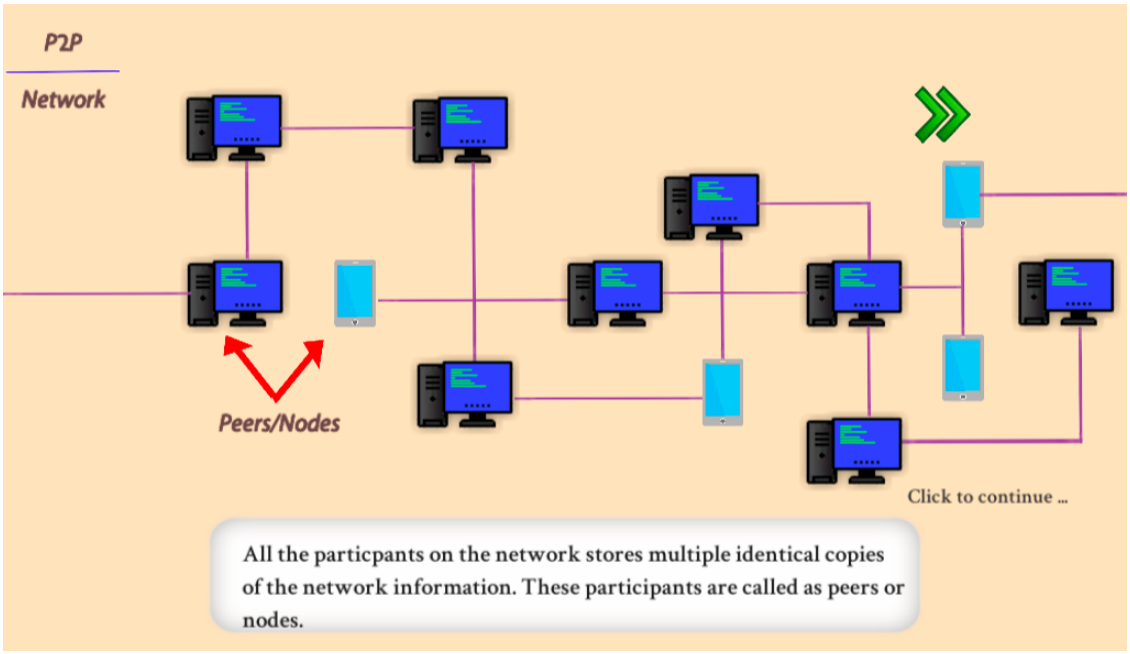

Figure 2.22. Blockchain concept explanation.

At the end of every quiz you receive a score given by the right and wrong answers (see Figure 2.26).

- Sensitive data exposure: in this game, the theory of HTTP and HTTPS is explained, then a couple of examples show how HTTPS is more secure than HTTP. After that, lines of code are added to the user (see Figure 2.27) to make an HTTPS connection. To do this there are suggestions that allow a user with little knowledge about it, to achieve his task.

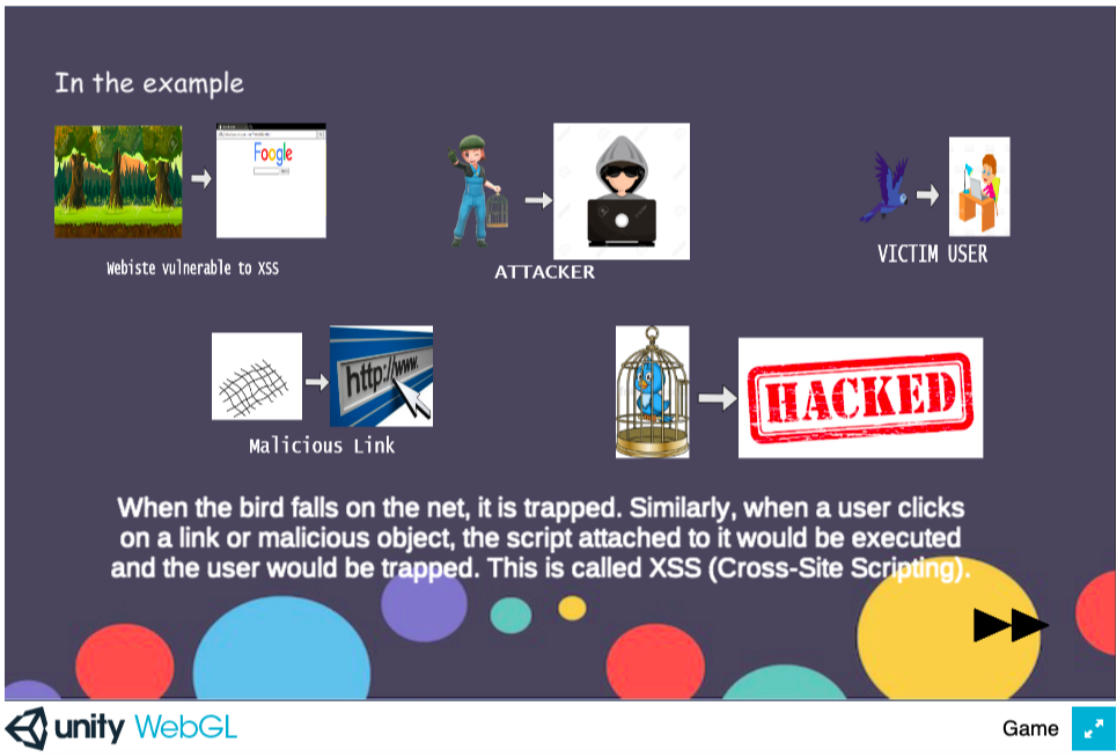

Figure 2.23. Explanation of XSS attack.

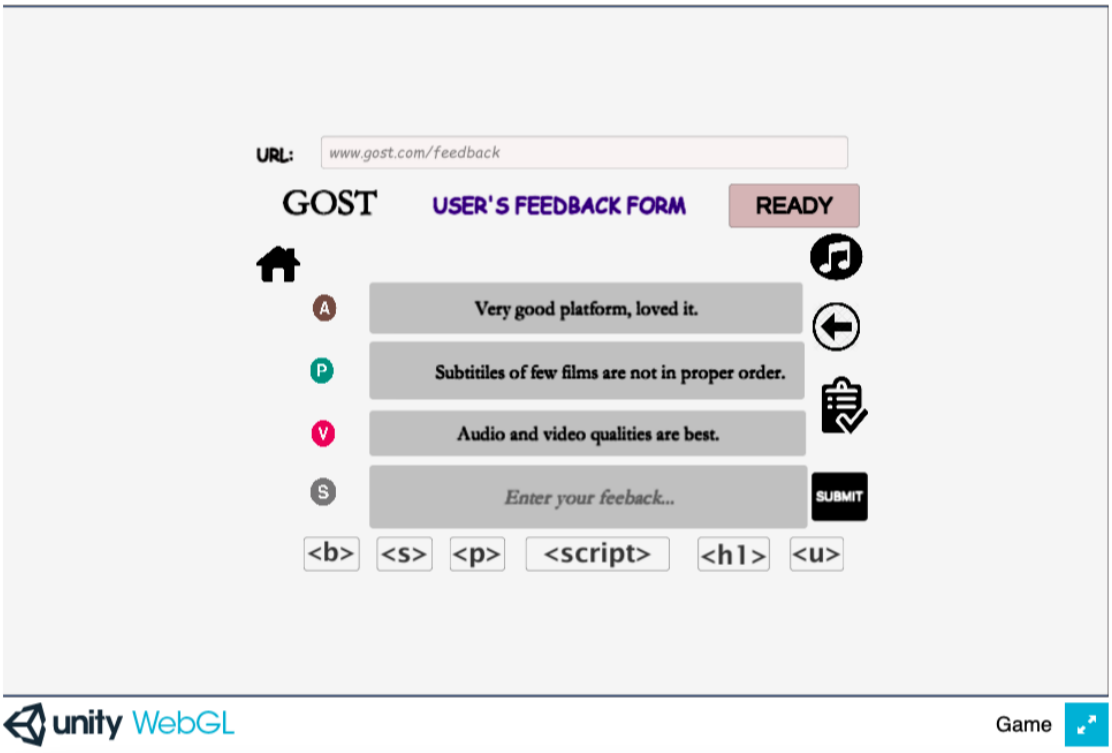

Figure 2.24. Web Site with possible elements for an XSS attack.

Below is a group of games that are still in an early development state and would like to cover a few topics:

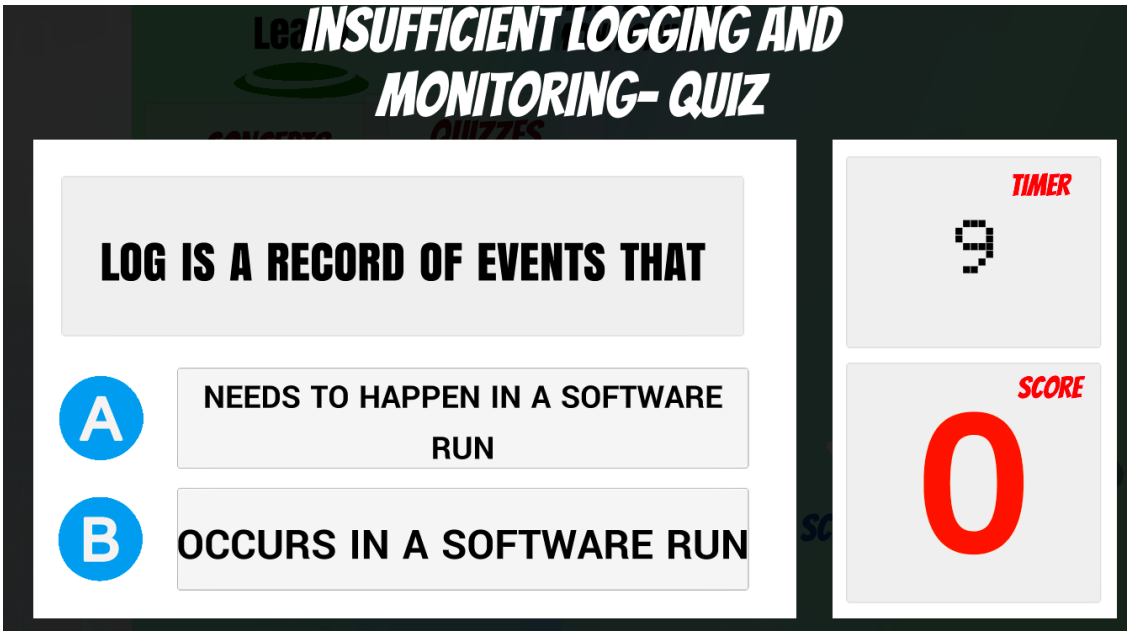

Figure 2.25. Quiz example.

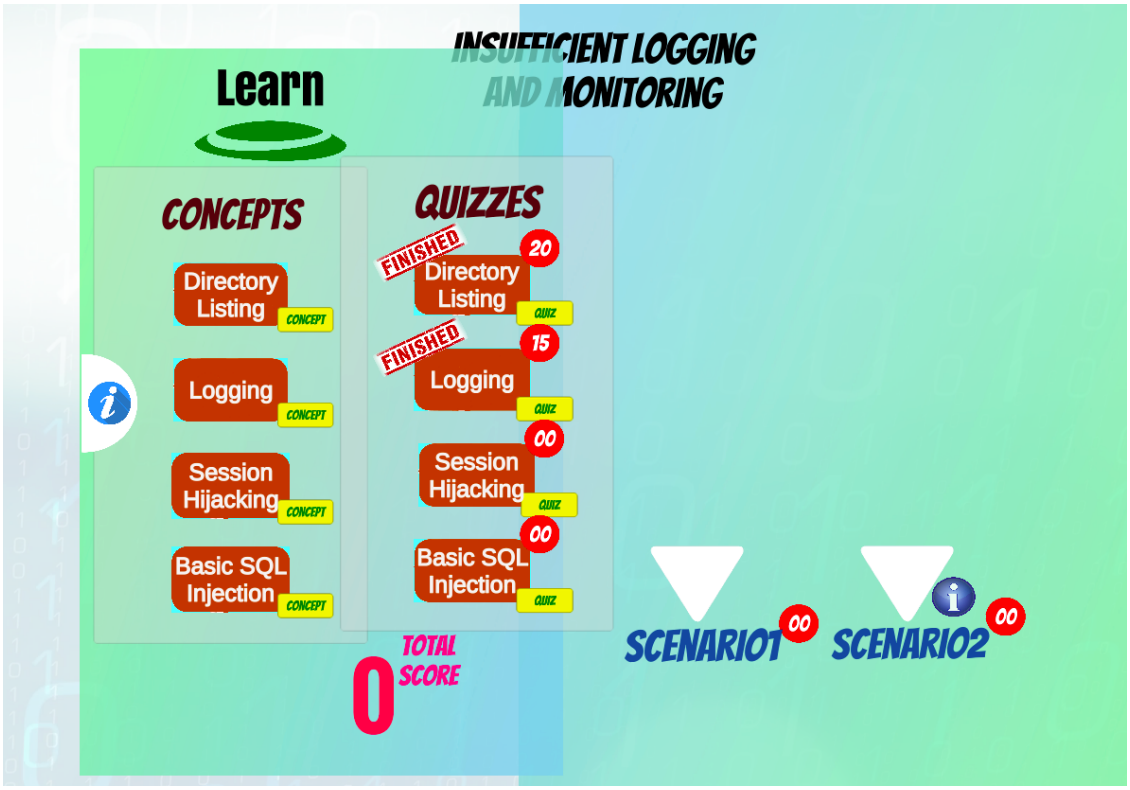

Figure 2.26. List of quizzes with relative scores..

- malware incident forensics;
- cyber crisis management plan;
- password management;
- incident handling.

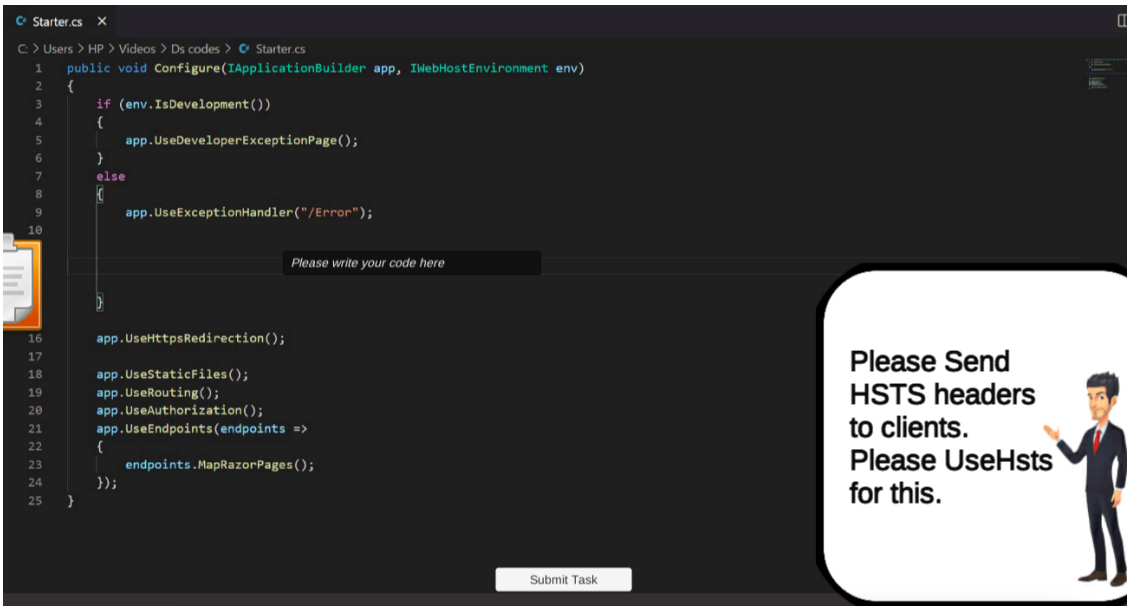

Figure 2.27. Code to complete for an HTTPS connection.

2.5.10 Interland

Web Site: https://beinternetawesome.withgoogle.com/it_it/interland

Introduce a very young audience to the world of the web, focusing in particular on the dangers that moving online can entail and on the behaviors to be followed or avoided in the contexts of social networks or digital payments. This game is adapted for a young audience. It's easy to play, and the simple and intuitive graphic is very helpful. The suggestions and indications are always present and explain in the best way what needs to be done.

To maintain a young target and also adapt this game to the anti-malware theme, a fifth world could be created in which the main character must avoid traps (pop-ups, phishing emails, etc) for not to lose points. While taking some items (like a computer, which indicates the software update) the character increases its score. This part of the game can lead young people to pay more attention when pop-ups open while browsing or to not immediately trust emails that may seem harmless.

2.5.11 Targeted Attack

Web Site: http://targetedattacks.trendmicro.com/

The game is a visual novel consisting of short videos in which the actors participate, interspersed with sections where the player has to make a decision. This allows the game to be very immersive and realistic, and to have a good number of alternative scenarios.

2.5.12 Data Center Attack

Web Site: https://resources.trendmicro.com/datacenter-attack.html

The game is made by the company TrendMicro, which deals with IT security in the corporate environment. The purpose of the game is to show potential buyers, but not limited to, the area in which the company operates, emphasizing the usefulness of managing corporate IT security with clarity and competence.

2.5.13 CyberSecurity Lab

Web Site: https://www.pbs.org/wgbh/nova/labs//lab/cyber/research

The player must manage the growth of a new social network and consequently defend himself from a series of increasingly sophisticated attacks against his start-up. The gameplay is made up of minigames that deal with different themes. This game aims to:

- teach how to defend your personal information in the digital world;
- identify phishing attempts;
- learn programming basics;
- defend against cyber attacks.

2.5.14 Stix and Stones

Web Site: https://github.com/dagerikhl/ddsg

It is a "defend the tower" type game in which the player has to defend 3 entry points from enemy attacks: client, network and server. Depending on the type of attack, the player must deploy the appropriate defense to neutralize it, because only certain defenses are effective in stopping an attack. In gameplay certain turrets (defenses) are capable of hitting only certain enemies (cyber attacks).

2.5.15 Netsim

Web Site: https://netsim.erinn.io/

It is a computer network simulator, in which it is possible to send and receive packets within the fictitious network (see Figure 2.28).

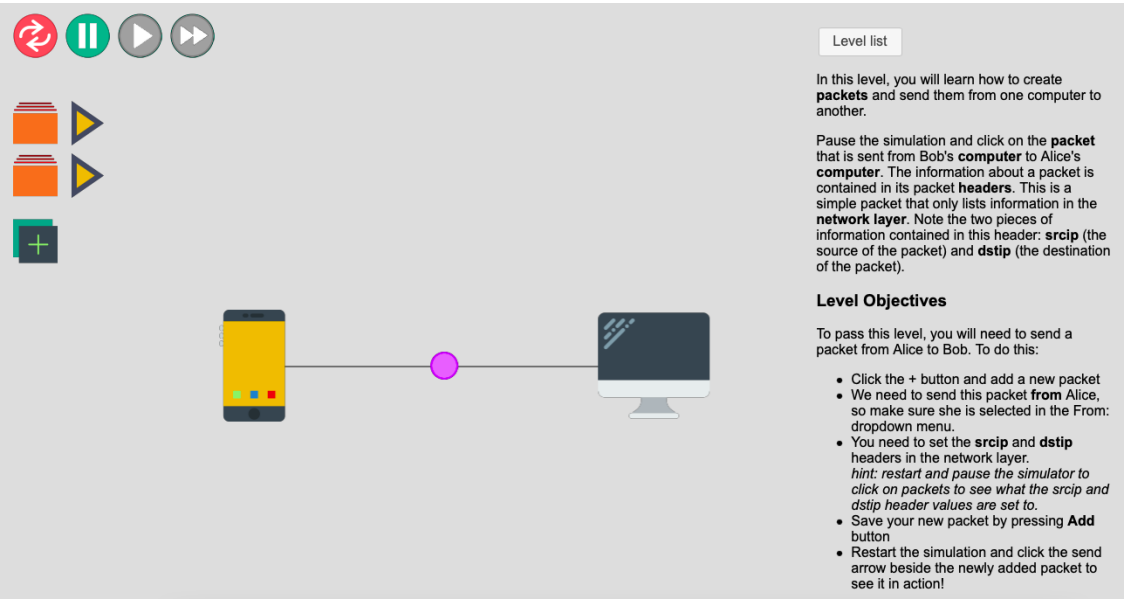

Figure 2.28. Packets exchange between two hosts.

To adapt this game to the Anti-Malware theme, it is possible to introduce new "entities" who takes the bad guy role. In this way the users can see the possible traps that they can meet during the navigation.

2.5.16 Permission Impossible

Web Site: https://groups.inf.ed.ac.uk/tulips/projects/1617/PermissionImpossible/

The game is very simple and is divided into a series of levels in which the player has to build the input and output rules of a firewall, following the indicated requests. To do this, bricks must be dragged in a row to form the aforementioned rules.

2.5.17 The Weakest Link

Web Site: https://www.isdecisions.com/user-security-awareness-game/

The protagonist is a new employee who has just started working in the company and the player has to answer a multiple choice question every working day for a month. Each answer is communicated whether the selected one is correct or not, with a brief explanation of its implications (see Figure 2.29).

In my opinion this game is efficient to reduce the IT ignorance, in particular against Malware. The user is as if he were inside the working environment, like in the office and is subjected to daily tests: fake email, form grabbing, dangerous calls, etc.). Answering the questions, the user learns some skills to avoid Malware and in case the user wants to deepen about something in particular, there is the "Read More" button.

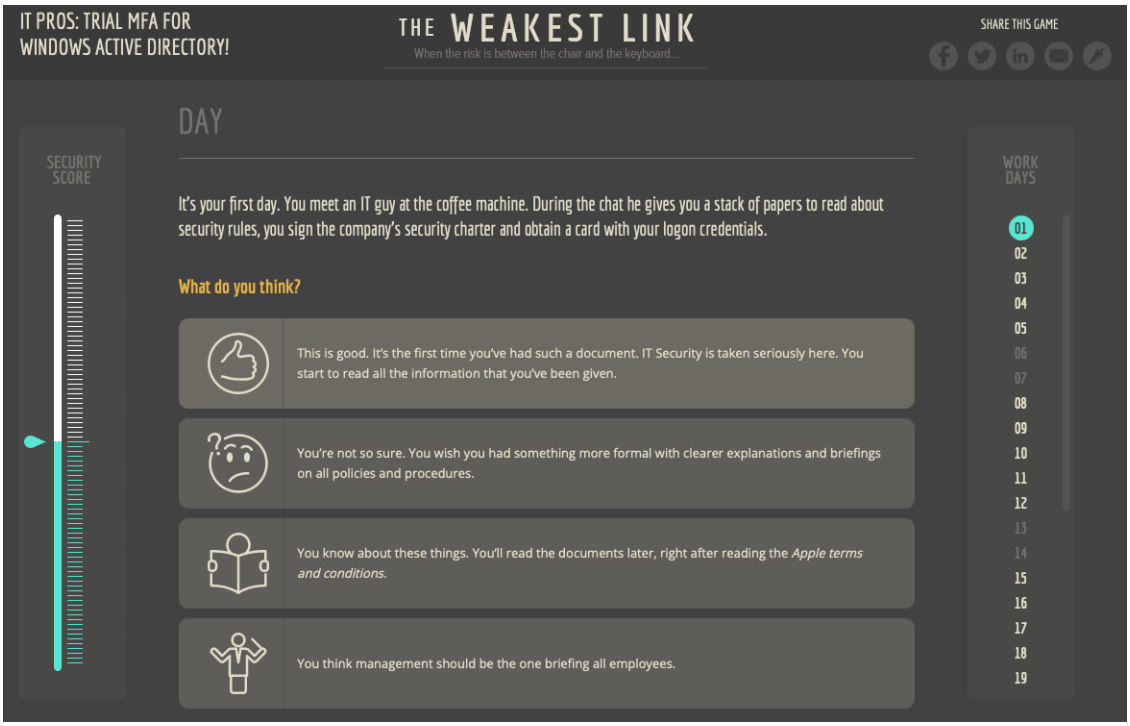

Figure 2.29. Kind of a question example.

2.6 SSG Analysis

From the analysis of the various SSGs present online, it emerges that some topics of the Cyber-Security course are covered, others are only partially covered and some are not covered.

One of the topics that SSGs cover is cryptography. In particular, there is Crypto Club which introduces notions of cryptography (encryption and decryption). However, this topic has not been explored in its most technical part, thus maintaining a target of users with basic knowledge

of cyber security. The various algorithms are not covered, but only examples are given where multiple characters are added, moved, or replaced to make them unreadable. To extend these games, technically speaking, it is possible to introduce a section for more experienced users where the various symmetric and asymmetric encryption algorithms are used.

Then there are SSGs instead which are set within the company and which help better to understand what dynamics there may be during a working day. These SSGs are Centrigrade, The Weakest Link, and Fintech Tycoon. The main differences between these SSGs are that:

- The Weakest Link deals with the topics only in theoretical form, in fact, the game has been designed and built as a collection of quizzes to which the user will have to answer and from each question, he will receive information and theoretical notions about it;
- Centigrade, on the other hand, deals with IT security both for the company and for personal security. For example, there are sections in which the player must collect as much information as possible from other people's social networks to try to carry out a brute-force attack on their passwords. This is used to put the user in mind when he is in front of providing data to social networks. As for the security of the company, however, there is a scenario in which the user must first create and then later identify fake emails. While in another level it is the management of documents, that is, the user will receive documents and must direct them in the way that he thinks is the best (trash can, send it via secure email, share it on social networks, etc).
- Fintech Tycoon, on the other hand, is more about managing the economic aspect of a company. Because the user must invest the company's money and resources in the best possible way to build up good defenses against cybercrime. But rather than specializing in technologies, the user will learn how to best optimize resources and then invest in corporate structures and technologies.

There is also a game that deals with computer networks, thus exchanging packets between different nodes. This is the case of Netsim, a computer network simulator that helps the understanding of the various packet formats with the fields that compose them. Furthermore, by playing Netsim you understand the mechanisms and the functioning of some communication algorithms.

Finally, there is Minigame Security which, in addition to covering some of the topics mentioned above, also deals with Firewalls, BlockChain, and some types of attacks such as SQL injection and Cross-Site Scripting (XSS).

2.6.1 Privacy Regulation, GDPR

From this analysis, it is clear that a topic of central importance that is not dealt with within the SSG, if not in a small part, is privacy, which has become increasingly important in recent years, especially after the introduction, on May 24, 2016, of the European Regulation, the GDPR (General Data Protection Regulation) - which repeals the twenty-year Directive 95/46 / EC on the protection of personal data and supports the national legislation on privacy contained in Legislative Decree 196/2003 (Privacy Code).

The adoption of the new Privacy Regulation was intended to create a harmonized legal framework and ensure uniform application of the rules on data processing throughout the European Union, develop the single European market, and strengthen the protection of the rights of the interested parties.

The benefits of having a single regulation in Europe are enormous.

Think of a company that operates in Spain and offers services or products that are then sold, perhaps online, even in Germany. In the absence of unified legislation, the company would have had to comply with both Spanish and German privacy laws. With the Regulation, this will no longer happen as each European state will have a harmonized discipline [15].

A possible solution to introduce these topics within an SSG is to make the user experience the working dynamics in which he finds himself having to make changes to ensure that the company

complies with the European legislation of the GDPR. Then make it involves the management like in Centrigrade, but also the modification, and deletion of data, making the company suitable for the new legislation.

2.6.2 Phishing

One of the most frequent issues is also phishing. The various SSGs, try to teach the user when to trust or not the email they receive every day. Phishing is becoming more and more current and of interest to companies, in fact, over the last couple of difficult years, businesses worldwide have been forced to accelerate their adoption of new technologies and IT security, and the cybercriminals have been just as fast to catch up. Here are some headline stats about phishing that you need to know for 2022.

Important phishing statistics for 2022:

According to IBM's 2022 Cost of Data Breach Report, the use of stolen or compromised credentials remains the most common cause of data breaches. They were the primary attack vector in 19% of breaches this year, a tiny drop from 20% in 2021. The report also states:

Stolen or compromised credentials were the primary attack vector in 19% of data breaches this year. 2022 has seen a tiny drop in this statistic from 2021, wherein stolen or compromised credentials were the primary attack vector in 20% of breaches. Breaches caused by stolen or compromised credentials had an average cost of $4.5m. This type of breach had the longest life cycle, 243 days to identify the breach and 84 to contain it. This length of time is 16.6% greater than the overall mean time for identifying and containing a data breach. Phishing was the second most common cause of breaches at 16%, costing $4.91m.

IBM's 2021 research cited a 2% rise in phishing attacks between 2019 and 2020, partly driven by COVID-19. CISCO's 2021 report echoed this, stating that at least one person clicked a phishing link in around 86% of organizations.

These attacks seem to be getting more frequent into 2022, too. In the first quarter of 2022, the Anti-Phishing Working Group (APWG) observed 1,025,968 total phishing attacks. This is the first time the quarterly total has exceeded one million, making it the worst quarter APWG has ever observed [16].

For these reasons, phishing is one of the most popular topics within this branch of the SSG. Because through the game it is possible to transmit concepts of fundamental importance nowadays within companies. This also allows for safer management of our data, which is often stolen and dispersed on the dark side of the internet.

In the SSGs analyzed, as mentioned above, some concern phishing but in a different way from the solution developed by me. In particular, The Weakest Link generally covers much of this topic but only theoretically through quizzes. While in my solution there are practical examples that make the game interactive and set in real situations. While in Centigrade, where interactivity is present, some aspects of phishing that I try to fill within my game (for example baiting, honey pot, and advertising pop-ups) are not addressed, but within it, there are only examples of fake emails.

Chapter 3

Applications

3.1 SSG Server

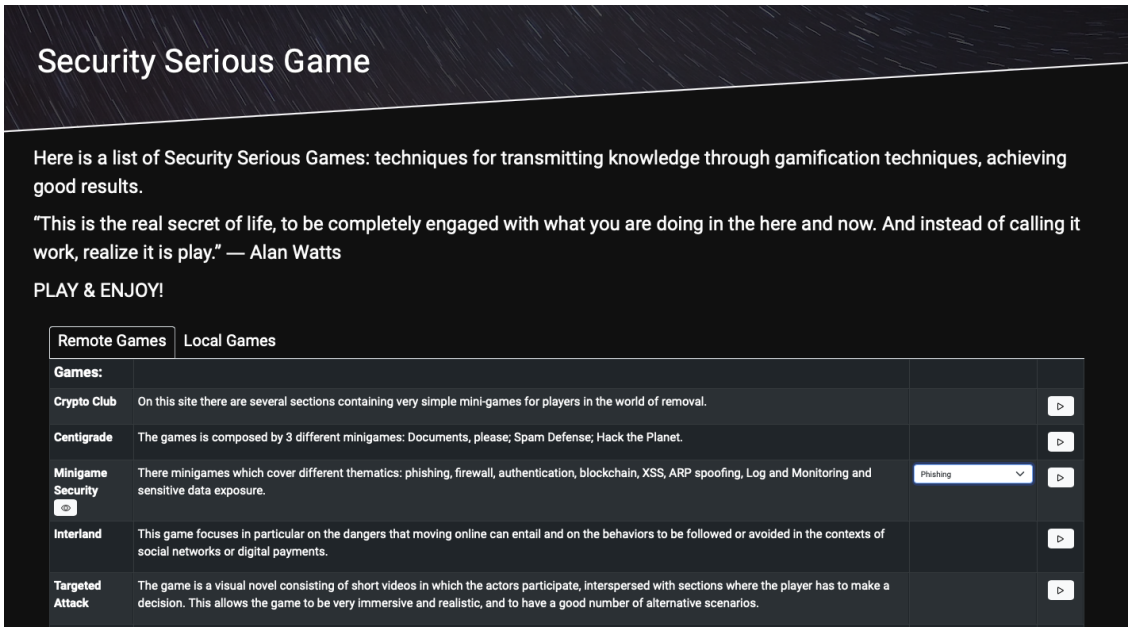

Figure 3.1.

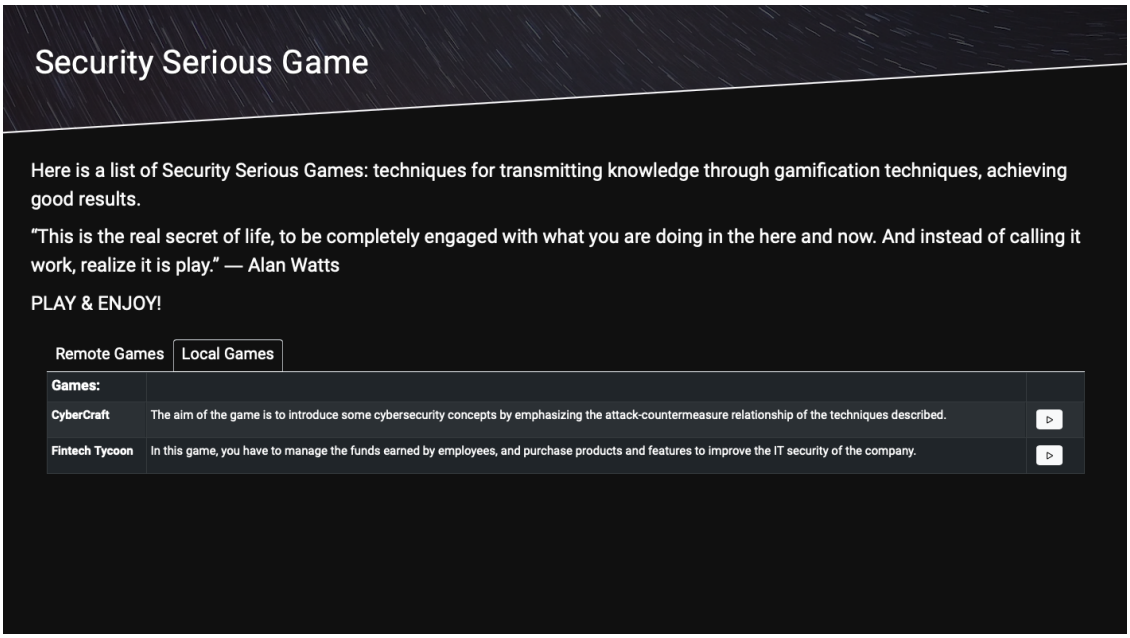

Figure 3.2.

3.1.1 Server: Idea and Advantages

I worked on this server to concentrate all resources in one "hub". The usefulness of this server is many:

- as mentioned above, the basic idea is to have a collection with all the various SSGs found on the web, making their playability easier and more comfortable. In this way, the user only has to read the description of the various games, and according to his preferences or what interests him, through the play button he can start playing that particular game;
- secondly, this work helped me to have a clearer idea about SSGs in general. Through their study, I was able to compare different designs and see their strengths and weaknesses for each. Furthermore, I could see through their analysis, the topics that are covered or not by the SSGs present in the server. And also based on this analysis, I was able to choose what to focus my game on;
- moreover, the creation of this server has the purpose of disseminating the existing SSGs. In this way the SSGs have more visibility users after having finished playing an SSG, always in the server interface can try others simply and intuitively. The diffusion of these games is very important, because their purpose is to teach the concepts of computer security, and each of them deals with different and very important issues.

3.1.2 Server: Design and Technologies

The server is represented by a table. Each row of the table is composed of name of the game, a brief description of it, and the play button that allows the start of the game itself. In the case of "Minigame Security", on the other hand, there is a button next to the name that allows visiting the website with the collection of various games, and a selection through which you can choose a game, and pressing the play button you can start.

In the server, there is also a tab that allows the remote/local games to switch. The local games were downloaded and installed directly on the server. While remote games are links that refer to assets on another device.

The technologies used for the graphic part (front-end) of the server are HTML and CSS and in particular the Bootstrap library, which is the most popular CSS Framework for developing responsive and mobile-first websites.

For a future project, the server can be expanded with new games that will be uploaded to the web. While as regards the graphic part, to make it even more intuitive, two significant words can be added next to the description to make it clear.

3.2 BE mAlWARE

3.2.1 Title

The game title came out of the similarity between the words Malware and Aware. Malware because it is used precisely to spread concepts regarding Malware, while Aware because you have to be very careful, since in many cases criminals exploit the ingenuity, emotionality and distraction of the human being.

So the title makes it clear how the game serves the user to be prepared when faced with situations where there is the possibility of spreading Malware.

3.2.2 The Idea

"Cyber attacks on Public Administration have always been a problem for various local authorities and 67% of public domains present "serious problems" of security."

Thousands of cyber attacks are carried out every day through the most varied techniques and terms such as malware, ransomware, and email phishing, have become part of the vocabulary even for the layman.

Cyber attacks on Public Administration have always been a problem for various local authorities. In recent years, the overall number of attacks and incidents related to cyber security in the PA has increased exponentially.

Even in the past year, we can recall several attacks, including:

Municipality of Brescia: on March 30, 2021, a ransomware hacker attack on various systems in the municipality made it inaccessible, for several days, to access the databases that manage tenders, building practices, the school system, the registry office, thus putting in difficulty the work of many offices.

Lazio Region: on 30 July 2021 a cyber attack compromised the use of some of the services and applications available to the citizen and seems to have started from the violation of an employee's user.

Lombardy Region: on October 15, 2021, a hacker attack aimed to overload the servers of the Region, sending them haywire with an accumulation of requests, or what we call a DDoS attack, Distributed Denial of Service. The intervention of the cyber security team ensured a very rapid resolution.

Still, on the subject of cyber security, Agid published the results of the tests conducted in December 2020 and required by the three-year plan for IT 2020-2022, which identified that 67% of public domains have "serious" security problems. A strong criticality if we consider that the access point to digital services is institutional portals, which can become the gateway to ransom attacks [13].

However, the human factor remains the main actor in the prevention of infections and should not be underestimated. For this reason, it is necessary to implement all possible preventive actions, designed to mitigate the risk of human error exposing the entire administration to high IT risks.

Therefore, adequate training of operators is essential, who must necessarily possess the basic knowledge to identify possible threats, promptly isolating them and preventing them from spreading further [14].

The idea of the game is a "substitute" for the training courses on computer security for the employees of the Public Administration. The advantage of using this game, rather than the classic training/refresher course, is interactivity. In this way, the learning is less boring and the duration is also drastically reduced, since with a course it takes hours to learn some theoretical notions, while through the game and therefore through practice the learning is more immediate.

In addition, there may also be a reduction in costs related to the transmission of information security concepts (see Figure 3.3).

The cost of Security Awareness Training is impacted by the number of users, languages in scope, type of training, and number of training courses. In evaluating the cost of Security Awareness Training, many industry analysts point to the TCO (total cost of ownership). The TCO for a Security Awareness Training includes the methodology and approach used, experience of the test creators, and quality of the end product. The starting cost for a typical Security Awareness Training program for a business with 50 employees is $1,000. Managing the cost of a Security Awareness Training is of course very important, but Security Awareness Training must follow a sound approach, with experienced trainers to provide value to the organization [17].

Figure 3.3. Security Awareness Training Cost.

From the moment in which there is no longer a need for a figure who has to teach, you go to save money that the company can use differently, also wanting to improve the infrastructures devoted to IT security.

Through the game, it is possible to learn how Malware spreads and in case of an attack, how to counter it. I thought about diffusion techniques because prevention is the first defense, and since once the cyber attack has caused damage and the system is compromised, the data is often lost and willingly ends up a short time on the "dark" side of the web. In addition, I also thought about how to counter the malware, so that users are not unprepared in situations where they are "under attack".

The various diffusion techniques that will be faced during the game are:

- Social Engineering: Baiting, Phishing, Pretexting and Scareware;
- Unattended USB stick;
- Click on a pop-up or banner;
- Visit infected websites or peer-to-peer networks;
- Connect to unsafe networks (honey pot);
- Downloading of software from untrusted sites;
- Software Vulnerability;
- Backdoor;
- UAC Bypass: to scale up privileges;
- Mobile apps downloaded from unofficial app stores.

3.3 Design and Technologies

3.3.1 React

As for the choice of technology for the development of the game, it fell on React. This allows you to make the SSG accessible from the Browser. The advantages of using this technology are:

- Declarative: React makes it painless to create interactive UIs. Design simple views for each state in your application, and React will efficiently update and render just the right components when your data changes. Declarative views make your code more predictable and easier to debug;
- Component-Based: Build encapsulated components that manage their own state, then compose them to make complex UIs. Since component logic is written in JavaScript instead of templates, you can easily pass rich data through your app and keep state out of the DOM.
- Learn Once, Write Anywhere: We don't make assumptions about the rest of your technology stack, so you can develop new features in React without rewriting existing code [18].

Moreover, thanks also to the "npm run build" command offered by React, it was also possible to deploy the game on a server provided by Politecnico. This allows the user to access the game via the browser through the IP address of the server itself. In this way the user does not even need to install the game on his PC to be able to use it.

3.3.2 Design

The source code is organized in such a way that if a developer wants to work on it, he can find his way around easily. This is because the organization of the various folders is very intuitive.

Starting from the src folder, there is this subdivision:

- **components:** this folder contains the components that are often reused on several levels. These components have been made parametric so that they can be reused in the various classes only by changing the parameters they take. Among the most used components is the GameWriter, which was used in the various levels to tell the story of the game, and only by changing the text element, different texts are displayed;
- **dnd:** here are all the classes used for the representation of Drag and Drop. This library was fundamental to making the game interactive and creating new simple and intuitive scenarios. Inside this folder there are the files: Box.js which are the draggable elements and Dustbin.js which are the elements where the boxes can be dropped;
- **img:** here are all the various images used in the game. To make the game simple and personal, some elements within the game have been hand-drawn using a tablet. Through these drawings the game is stylized and has a minimal style;
- **level:** this folder contains the various levels, and for each level then there will be different scenarios that are placed inside the scenarios folder;
- **scenarios:** here, on the other hand, there are other folders with various levels. This is because within these folders there are the various scenarios that make up the different levels, with their dynamics and the various actions that the user must perform to complete the level;
- **view:** this folder contains the initial view, that is the initial screen of the game; and the view that appears during the entire duration of the game (the external part of the screen, where the current level, the score, and the time are present).

3.3.3 Contest of the Game

The choice of this game is due to the analyzes carried out previously and the use and study of the existing SSGs present within the Server. As we have seen above, the statistics speak of a sharp increase in cases of malware spread within the public administration. This is why the game is sought within a municipal office. The plot is about John, an employee of the fictional Cyberlandia municipality who is about to start a new working day. The choice of the municipality is due precisely to the large number of data stolen in the Public Administration. As for the interaction

between the user and the game, there is a narrator that will accompany John for the duration of the game. For this technique I took inspiration from the various SSGs tried previously. This is an efficient technique because it does not make the player feel alone and bewildered, it also makes the gameplay simple and intuitive. In fact, in every choice that the player will have to make, the narrator will explain which are the various options to be taken and in which way they will be taken.

As a target, I chose the employees of the public administration. This is because these employees are often subjected to training/refresher courses regarding IT security and, as already mentioned in the previous chapters, through the game these notions are made less boring and allow a considerable saving in economic terms by the company.

3.3.4 Game Structure

As for the organization of the game, the game is divided into levels. In each level, the player will face situations in which personal and corporate IT security is put to the test.

For each level, there are different danger categories. For example, the first level deals with the phenomenon of Baiting. That are situations in which the user's curiosity is put to the test and in some cases, it is exploited to obtain data or access to personal resources. I thought about Baiting because in games it is not treated except in quizzes, so situations without a plot or an association with real life.

On the second level, on other hand, we talk about phishing through emails. This is because the statistics studied and reported in the previous chapters highlight how the spread of malware in most cases occurs through fake emails. At this level, the user will therefore have to recognize the true emails from the false ones.

In the third chapter, on the other hand, the honey pot and software vulnerability are dealt with. In fact, in many cases, the user receives software or OS update notifications during working hours. In this case, the player will have to decide whether to update the OS immediately or postpone the work he has to complete. This level was designed to warn employees, given that many times updates are slow and demanding and therefore are often postponed to a later date without taking into account the risks that can be run. While in the case of the honey pot, the user is faced with the choice of continuing with the municipal network or experimenting with new free networks to see if they are better in terms of speed. I introduced this part because users often tend to trust free networks, but unfortunately, these are not always reliable they are only trapped to steal sensitive data.

The fourth level, on the other hand, concerns the dangerous aspects of internet browsing, such as pop-up advertisements, which are often misleading and have not been dealt with in the SSGs tested so far. Or the download of software from untrustworthy sources and the UAC Bypass used by the bad guys to have access to sensitive sections and data. These aspects have also been introduced into the game because they often occur in administrative environments and in addition to being seen from the point of view of theory, they have never been addressed in practice in computer security games.

During his adventure, the player will be accompanied by the time of the day, which helps to make the dynamics of the working day real so that the player can feel like they are living a typical day at the office while playing; and at the bottom right of the game screen, by the score: this will increase more each time the user gives a correct answer, while there will be no increase in the case of wrong answers.

At the end of the game, the user will be shown a report with the various correct answers and incorrect answers, and will also be able to see the total points he has scored. Reporting is a very popular strategy in SSGs and that is why I have chosen to use it in my game. Furthermore, thanks to the report, it will be possible to establish knowledge bands to understand the average level of employees of a particular company. To take measures if the level is not sufficient to ensure the safety of the company itself.

The choice of the structure of the game is because I believe it is good for spreading this type of knowledge, that is computer science. The user playing is as if he were in the office in front

of his PC, and facing the situations that arise in the various levels, he will be ready when these happen, if they should happen. So the likelihood with real life, the narration that accompanies the player throughout the game, and the various issues that had not been addressed before are the strengths and the reason for the success of spreading the cybersecurity concepts in companies.

Chapter 4

Results

4.1 Results

4.1.1 Knowledge Survey

To test employees' computer skills before releasing the game, a multiple-choice quiz was given. Within the quiz, the main topic is Malware: how to recognize certain types of Malware and also how to mitigate them.

The questions in the quiz are available in Appendix A, and the contents are:

- phishing: so what to do in case of receiving unverified emails, and try to understand if the content is reliable before doing what it says to avoid the spread of Malware inside your PC;
- avoid the traps present on the web, such as clicking on an advertising pop-up, or downloading only Software from trusted sources;
- make the relationship with your PC safer, limiting access by third parties (for example apps that request consent to use our data), or select before browsing, only Wi-Fi networks of which you know the source.

The statistics belonging to the questionnaires show that there have been improvements in what concerns the understanding of the concepts by the users. In fact, before the game, only 24.4% of users knew that malware could spread via USB sticks, while after using the game, 66.7% of users were aware of this, about triple. Another statistic that sees a less significant improvement, however, is that concerning clicking on links within emails without first being sure of the source, which sees an increase from 78.8% to 96.7%. Before testing the game, only 54.5% knew that human ingenuity is a factor in the spread of Malware, compared to 76.7% after. The same statistics and same results were for users who previously thought that the web was a safe place and not a stage for the spread of malicious software. Instead, it has gone from 75.8% to 86.7% of users who update the software on their PC for security reasons.

4.1.2 Game Feedback

Here are summarized the main aspects commented by the players.

Utility of the game

The basic idea of the game was appreciated. The various levels are well structured, to better disseminate knowledge on IT security. Furthermore, the game has been called useful because, through its simplicity, the concepts are easy to learn. Therefore, once the user has used the game, he should be able to recognize the various dynamics of cybersecurity to avoid, for example, the spread of malware.

Gameplay

The game was defined as very simple and intuitive. No particular difficulties have been encountered in its use by users. The use of quizzes on some levels simplifies the dissemination of theoretical concepts even more but at the same time, being set in a real dynamic, it also helps with learning the practice. For some users, with more basic knowledge, however, some levels were too simple. But overall, the game has helped them increase their background when it comes to cybersecurity. Some users would have preferred the second-level emails to be written with a PC, while some liked the handwritten style because it was consistent with the scenarios and drawings of the other levels

Game Story

The idea of a game set within the company during the working day helps in the identification of the user in real everyday life. This helps in case one of these situations occurs in reality and makes the user ready to face this dynamic in the best way and above all in a safer way. One aspect that has been found and that could have improved the game's storyline is the interaction with colleagues. To make this experience even more real, given that during everyday life it often happens to interact with one's colleagues or with one's bosses.

Chapter 5

Conclusions

5.1 Conclusion

5.1.1 Malware Knowledge and SSG Status

The central topic of this thesis and the research behind it are malware. Over the years this phenomenon is growing more and more, and one of the most effective ways to combat it is the dissemination of knowledge in the field of cyber security. In this thesis, the research has focused on Security Serious Games, but lately, other effective techniques have been introduced with the same purpose. For example, there are the CTFs (capture the flag) that are becoming more and more popular, and the users who participate in them become more and more passionate.

Capture the Flag (CTF) competitions combine playful activity with the more traditional teaching of cyber security and are becoming increasingly popular. They constitute a digital reinterpretation of the flag-stealing game, where the various teams aim to conquer the flags of the opposing teams and protect their own. In the digital version, the flag is replaced by a code, generally a sequence of alphanumeric characters that are difficult to predict [19].

So it can be said that to avoid the spread of malware and to make this rapidly increasing phenomenon slow down, more and more new teaching techniques are emerging. We try to make these teachings less and less boring through initiatives such as that of the SSGs seen above. There are still many gaps to be filled, such as the effectiveness of these games, or topics that have not yet been covered by them.

However, it is important and auspicious to see how companies are investing more and more in these means of disseminating knowledge to make them safer.

5.1.2 BE mAlWARE: Future Developments

BE mAlWARE was developing with the idea of being widespread within the public administration. For this reason, it is adapted to a target of users with low-level IT knowledge, and to be suitable for this type of target it is very simple and some technical aspects are not explored. For this reason, among the aspects that can be improved, there is certainly that of making it more technical to make it understood in more detail the mechanism behind the spread of some types of Malware. This would help even more in countering some types of cyber attacks because it would make users more experienced.

5.1.3 Improvements

In addition to making the game more technical and thus moving the target towards more experienced users, other improvements can be applied. For example, in some situations, instead of

displaying alerts that say what is the best behavior to take in front of certain types of Malware, you could advance the story of the game, and show in practice what the possible consequences are of that Malware.

Another improvement could be the introduction of the active participation of some figures within the game. Such as, for example, dialogues with colleagues, or situations in which you interact with your boss or with customers. This is to make the dynamics of the game even more real.

Furthermore, the game is very simple, so you can improve both the graphic element, above all the logic component. That is, you can create logically more complex dynamics to make the game more intriguing and more complete.

5.1.4 Accessibility

The game is accessible via a browser by connecting to a server. There is therefore no need for installation because it has already been installed on the appropriate server.

From this point of view, the game could be made accessible via an app that can be downloaded on the PC, or a mobile app that can be played from your smartphone.

Furthermore, the game has been implemented in English, so we could think of a future version adapted to Italian.

Bibliography

[1] Kate Brush, Linda Rosencrance, Michael Cobb, "Cybercrime", https://www.techtarget.com/searchsecurity/definition/cybercrime

[2] What is Cybercrime?, https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

[3] Cyber Security Statistics, The Ultimate List Of Stats, Data & Trends For 2022, https://purplesec.us/resources/cyber-security-statistics/

[4] What is Malware?, https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html

[5] All about Malware https://www.malwarebytes.com/malware

[6] Alex Scroxton, Proofpoint's 2020 State of the Phish report https://www.computerweekly.com/news/252477228/End-user-security-ignorance-laid-bare-in-new-report

[7] Social Engineering, https://www.imperva.com/learn/application-security/social-engineering-attack/

[8] Yasin, Affan and Liu, Lin and Li, Tong and Fatima, Rubia and Jianmin, Wang, "Improving software security awareness using a serious game", IET Software, Vol. 13, No. 2, pp. 159–169, 2019, Wiley Online Library

[9] Game-based Learning and Gamification, 16 April 2020 https://www.savethechildren.it/blog-notizie/game-based-learning-gamification-e-didattica-cosa-sono

[10] The Bartle Test of Gamer Psychology - Gamer Types, https://www.gamify.com/gamification-blog/the-make-up-of-gamers-the-bartle-test-of-gamer-psychology

[11] Nick Yee, "Motivations of Play in MMORPGs", Results from a Factor Analytic Approach, http://www.nickyee.com/daedalus/motivations.pdf

[12] Security Serious Games Online, https://docs.google.com/document/d/1SIM8fnZw8J1U9sJiSFHkL88hNQLSz8J7i1AgCwOmD_M/edit

[13] CyberCrime on Public Administration, https://www.plurimedia.it/blog/come-proteggere-la-pubblica-amministrazione-dagli-attacchi-informatici

[14] Human Factor on Public Administration, https://www.cybersecurity360.it/nuove-minacce/ransomware/attacchi-ransomware-nelle-pa-cosi-si-garantisce-la-sicurezza-dell

[15] GDPR, https://www.ufficiobrevetti.it/che-cose-il-gdpr-introduzione-alla-nuova-normativa/

[16] Phishing statistics, https://www.egress.com/blog/phishing/phishing-statistics-round-up

[17] Security Awareness Training Cost https://www.trustnetinc.com/security-awareness-training/

[18] React Features https://reactjs.org

[19] CTF, What is it? https://www.agendadigitale.eu/sicurezza/capture-the-flag-diventare-esperti-di-cybersecurity-giocando-le-challenge/

Chapter 6

Appendix A

6.1 Survey

This survey is given to players before they start playing the game. Its purpose is to verify knowledge about IT security, in particular about Malware. Always the same survey was distributed after playing to see if there was an improvement in users' knowledge of computer security. All the questions used in the quiz are listed below, and the correct answer has been highlighted in bold.

(The survey was conducted in Italian for ease of understanding by users.)

Un malware puó

- **essere veicolato da softare installato su penne USB**
- essere trasmesso da app scaricate da playstore non ufficiali
- essere trasmesso da fonti diverse, quindi non é utile avere un anti-virus installato

Un attacco Malware puó:

- fare in modo che il PC della vittima si scarichi piú lentamente
- **fare in modo che dati sensibili della vittima vengano rubati**
- aumentare le prestazioni del PC della vittima

Alla ricezione di un'email contenente link

- **fare attenzione prima di cliccare sul link, quindi informarsi sulla fonte e sulla sua affidabilitá**
- non cliccare mai, in nessun caso
- cliccare e scaricare i dati associati al link ogni volta, senza nessun controllo

L'emotivitá e l'ingenuitá dell'essere umano

- vengono usati per creare pubblicitá che gli possano interessare
- **spesso fanno da tramite per la diffusione di software malevoli**
- non sono un fattore condizionante nell'ambito della sicurezza informatica

La navigazione nel web

- Ormai ha raggiunto livelli di sicurezza alti, che ti permettono di navigare sempre in condizioni di sicurezza
- **Spesso é palcoscenico di attacchi e trappole per la diffusione di Malware**
- é sicura solo se in possesso di un buon antivirus

Per ció che riguarda le comunicazioni

- Le email sono il mezzo piú sicuro
- **Le email possono andar bene, a meno che non si tratta di una comunicazione importante contenente dati sensibili**
- C'é sempre bisogno di almeno due vie di comunicazione (ad esempio email e chiamata telefonica)

Nel proprio PC

- **Sempre meglio avere tutti i software aggiornati per questioni di sicurezza**
- Si aggiornano solo i software che si usano piú frequentemente
- A meno che l'aggiornamento non é obbligatorio, conviene lasciare i software nella versione precedente per non occupare troppa memoria con gli aggiornamenti

Chapter 7

Appendix B

7.1 User Manual

7.1.1 Installation

At the time of this writing, it is not necessary to install the game to try it, as it can be played at this address. However, if the game is not available online, it is also possible to play it from your computer using a web server. The steps to follow are explained below.

7.1.2 Server Game Installation

To run the game you need to have an Apache web server installed on your computer. A solution for this point is to use the free XAMPP1 software, available for Windows, macOS, and Linux. After completing the installation it is necessary to locate the folder where the XAMPP files have been saved, which is generally:

- on Windows: C:/xampp
- on Linux: /opt/xampp
- on MacOS: /Applications/XAMPP/xamppfiles

Inside it, open the htdocs folder and create a new be_malware folder where the game files will be placed.

7.1.3 Building the Project

After setting up the web server you need to get the game files by downloading the GitHub repository at https://github.com/s275945/be_malware

(using the command git clone git@github.com:s275945/be_malware.git or by simply downloading the file.zip).

Then you need to enter the project folder with a terminal and run the 'npm install' command to download the necessary node modules (for the npm commands you need to install nodejs on your PC). Once the node modules have been downloaded, still staying inside the project folder with the terminal, run the 'npm run build' command. This command will create the 'build' folder and its contents must be copied into the previously created be_malware folder.

7.1.4 Run the Server and the Game

After performing all the steps described so far you need to start the Apache server from the XAMPP control panel.

To start playing, connect from your browser to the page http://localhost/be_malware.

Chapter 8

Appendix C

8.1 Programmer Manual

The source code of the game is available on GitHub at: https://github.com/s275945/be_malware

In this chapter I talk about the structure and the code used for the development of the game.

8.1.1 Structure

The game is structured as follows:

- Inside the **/src** folder there are all the subfolders containing the game code;
- The **/components** folder contains the JavaScript classes with the objects that are used several times within the game. For example there are: the GameAlert, which is used every time the user answers a question or performs an action and through an Alert he is told whether he has taken the correct action or not; or the GameHint is present, which instead is used within some levels in situations where the user has to make decisions and if he finds himself in difficulty, through this Hint he receives help to respond in the best way; and then there are other objects that are repeated during the game such as the AnswerButton (the buttons that the user needs to answer some questions), the GameButtonSkip and the GameButtonNext (used relatively to skip the scrolling of the narrative text and to change scenario), the GameWriter (which is the writing present in most of the scenarios to narrate the game) and the VerticalCenteredModal instead which is used in the initial screen to get more information about the game and which appears when the user clicks on the 'About' button;
- The **/dnd** folder instead contains the objects used to make the Drag and Drop within the game. The objects used are Boxes, which are the elements that can be moved, and Dustbins which are instead the elements where the Boxes can be released. Also in this case the objects are parametric, so that they can be reused in other scenarios if necessary and therefore simple to use for any future modifications;
- In **/img** there are all the images used in the game. Some images were taken from the web, while others were created via hand drawings on the tablet. The choice of images fell on stylized images, to make the game simple and easy for the user to understand;
- Inside the **/music** folder is the accompanying music for the game. In case you want to replace it, just choose a new bravo in mp3 format, rename it ringer.mp3, and replace it with the old file, and that's it;

- Then there are the central folders of the game. The first, the **/level** folder, contains the various levels of the game including the intro and the report. Within the various files in this folder, there are the various states and objects used within the levels. The files in this folder are containers of the scenarios used in the composition of each level and which are switched during the game;
- The **/scenarios** folder instead contains the scenarios that make up the various levels. In each scenario, the user must make decisions and consequently take actions to move forward in the game. In turn, for easier understanding, the /scenarios folder is divided into four subfolders, each for the various levels;
- Finally, in the **/view** folder there are the initial and final screens of the game. And the screen that accompanies the user throughout the game showing the time, level and current score.

8.2 Source Code

As far as game development is concerned, I used React as a technology. This is a JavaScript library for the user and web interface. Furthermore, the division into reusable components offered by React makes its use and the management of the classes used for the realization of the projects simple.

8.2.1 Routes

The first component to be rendered is the GameRouter. Within this component, there are various paths used in the game, and different components are associated with each path. The paths are inside the routesMapping[] vector and the components associated with the paths are scanned for rendering through the map instruction as you can see in the following code:

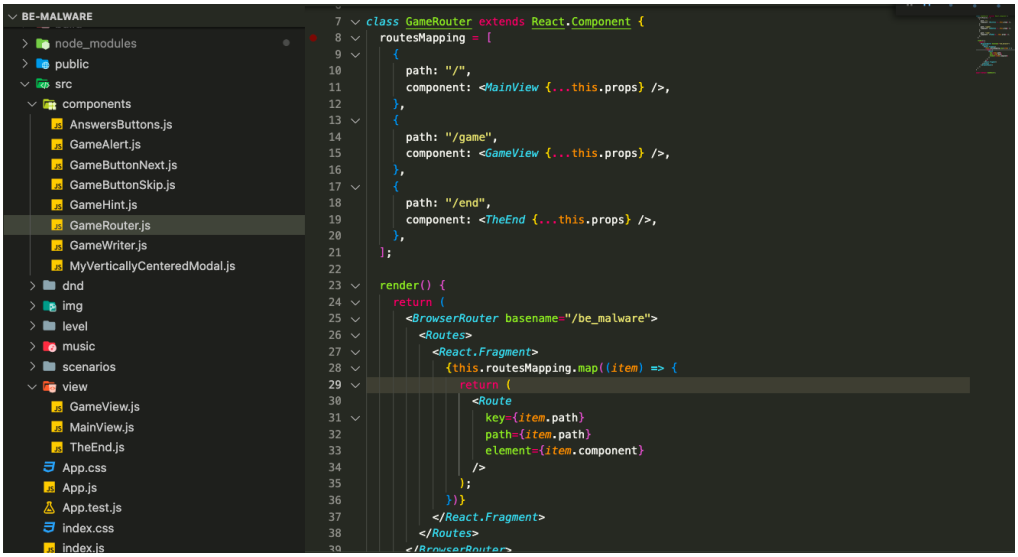

Figure 8.1. Routes.

The paths used in this case are: '/' or the starting path where there is only the Intro screen with the info about the game, '/game' which collects the various levels and scenarios, and finally '/end' which is the final screen of the game.

So the first component to be rendered is MainView. This screen has been designed to give an introduction to the game through a brief description at the bottom of the page, and for those who want more information, there is the 'About' button which will allow the appearance of a

Modal containing additional information. For example, the reason for this game is explained, as the setting and what the user will encounter.

8.2.2 Level Handler

Clicking on the Play button of the MainView plays the music that will accompany the user during the game and there will be a switch to the path /game. Once the Route has been changed, the first component to be rendered is the GameView.

This is the main component, within which there are different states for managing and rendering levels and for keeping track of time and score.

Levels are managed within GameView with a state variable called 'actualLevel' (initially set to the value intro), and with a switch within which there is a case for each level. Inside each case, a new component is rendered, and each component is passed the 'handleLevel' function to modify the actualLevel state variable. In this way, every time the actualLevel is updated thanks to the function, the new component belonging to that case will be rendered.

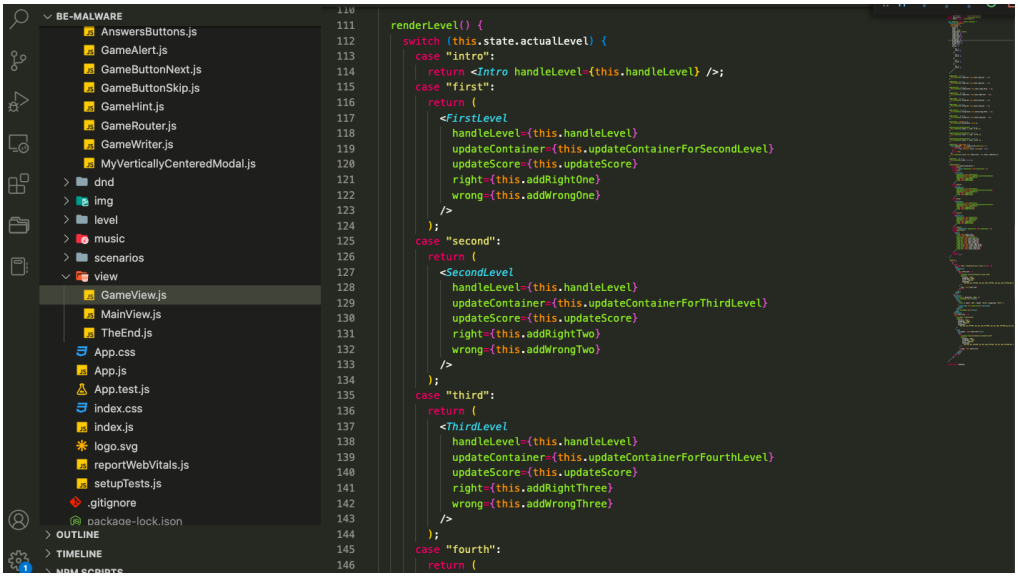

Figure 8.2. Switch case for handling levels.

Also, as anticipated, in GameView there are state variables to keep track of the time, the current level, and the score. The updating of these variables takes place through functions that are passed to the interesting components. For example, the last scenario of the first level which in this case is FirstLevelHacked is passed as a property of the 'switchToSecond' function which, in addition to updating the actualLevel state variable for passage to the next level, also contains the updateContainer() method which will update the state variables that kept track of the level and time in the game.

While, as regards the update of the score there are small differences. In fact, the function to increase the score is passed to all those scenarios where the user has to make decisions or perform actions. And only if the decision taken is correct, the updateScore() function is called which increases the 'score' state variable present in GameView.

8.2.3 Scenario Handler

Each level in turn contains more scenarios. Within each scenario, there is an introduction to the level, explanations of what the user will have to do within that scenario, and the consequences of the choices made by the user.

For the management of the scenarios, the same mechanism already used previously for the management of the levels has been used. That is, for each level there is a state variable called actualScenario and there is a switch case where, based on the value of actualScenario, one component will be rendered rather than another. To do this, the handleScenario() function is passed to the various scenarios as properties, so that every time it is called it modifies the actualScenario variable present in the level to change the switch case.

```
28  renderScenario() {
29    switch (this.state.actualScenario) {
30      case "intro":
31        return <FirstLevelIntro handleScenario={this.handleScenario} />;
32      case "choice":
33        return (
34          <FirstLevelChoice
35            handleScenario={this.handleScenario}
36            updateScore={this.props.updateScore}
37            right={this.props.right}
38            wrong={this.props.wrong}
39          />
e-malware/src/components/
js
41        case "leave":
42        return (
43          <FirstLevelLeave
44            handleScenario={this.handleScenario}
45            updateScore={this.props.updateScore}
46            right={this.props.right}
47            wrong={this.props.wrong}
48          />
49        );
50      case "dnd":
51        return (
52          <FirstLevelDnd
53            handleScenario={this.handleScenario}
54            updateScore={this.props.updateScore}
55            right={this.props.right}
56            wrong={this.props.wrong}
57          />
58        );
59      case "hacked":
60        return (
61          <FirstLevelHacked
62            handleScenario={this.handleScenario}
63            handleLevel={this.switchToSecond}
64          />
```

Figure 8.3. Switch case for handling scenarios.

8.2.4 Components

For the development of the game, it was necessary to use different components, which have been made adaptive so that they can be used on multiple occasions.

- AnswerButton for example is the component that was used in case the user has to decide between two possible options. To make it parametric I put two callBacks inside the onClick that are passed directly to it from the component that calls the AnswerButton and two labels that are the words inside the buttons. So for future projects, if you want to reuse this component, just change the labels and callBacks in the calling component.
- The GameAlert also made parametrically, is the information that is given to the user once he has acted. In this case, the parametric values are the head, which tells the user whether he has performed a correct action or not, and the text: the explanation of why the action taken was correct or not. If the answer is correct, the alert will be green, and vice versa, if the answer is wrong, it will be red.
- The GameButtonNext is the button used to switch from one scenario to another. Here the parameters that can be modified are the button label and the callback which is launched at the onClick moment.

- The other key component is the GameWriter. The editable parameter in this case is the text that will be shown to the user. Furthermore, inside there is also another component, the GameButtonSkip, which allows the player to skip the typing effect and be able to read the complete text directly. For this, a 'skipped' variable has been used and in case its value is set to false there is a typing effect, while once you click on the Skip button its value is set to true and the full text is in HTML format.