Raising Cybersecurity Awareness on Employees Through Serious Games

UNIVERSITY OF TURKU
Department of Future Technologies
Master of Science in Technology Thesis
Networked Systems Security
2019
Vasiliki Kirtsou

UNIVERSITY OF TURKU
Department of Future Technologies
VASILIKI KIRTSOU: Raising Cybersecurity Awareness on Employees Through Serious Games
Master of Science in Technology Thesis, 106 p.
Information Security and Cryptography
Networked Systems Security
December 2019

Nowadays, cybersecurity plays an integral role for everyone's online presence where extensive usage of computers, smartphones and other smart devices has become the norm. More specifically, businesses need to pay additional attention to it, since they are handling sensitive data of their employees and their customers on a daily basis. Many cyber attacks are incited by a human action done by mistake or negligence. Phishing and social engineering attacks are very often the initial attack vector and they are both targetting human weaknesses.

To fight this ongoing battle, personnel training on cybersecurity is of utmost importance. However, traditional training methods seem to have certain shortcomings which effectively impact negatively their teaching output. For this reason, in this master's thesis we examine serious games as an alternative way of teaching cybersecurity. A serious game is referring to a game whose primary purpose is not entertainment. Serious games have been gaining popularity lately as an educational or training method, and several companies have been created to cover the market needs for such.

This master's thesis presents two commercial off-the-shelf serious games which aim to raise awareness of certain cybersecurity concepts to employees, as part of their cybersecurity training. The first game, *Surf Clean*, focuses mainly on social engineering but also addresses general security principles that are fundamental for every enterprise regardless of its size. The second game, *Cyberzen Desk*, allows the player to experience the importance of correctly handling and protecting sensitive information and items, through a VR game.

Ultimately, we present the results of a user satisfaction survey on the latter, in which we saw very promising results overall. The participants seemed to embrace the new technology and were excited to have a serious game as part of their training campaign. However, we identified possible improvements concerning the content of the game, in order to help the participants relate more to it and as a result incease its learning effectivess.

Keywords: cybersecurity training, human element, serious games, commercial off-the-shelf

Table of Contents

Acronyms

Acronym	Description
3D	Three-Dimensional
ASCII	American Standard Code for Information Interchange
ATM	Automated Teller Machine
COTS	Commercial Off-The-Shelf
CTF	Capture the Flag
NPS	Naval Postgraduate School
OWASP	The Open Web Application Security Project
SAIC	Science Applications International Corporation
SG	Serious Games
URL	Uniform Resource Locator
UX	User Experience
VR	Virtual Reality
XSS	Cross Site Scripting

1 Introduction

In today's modern society, with the digitalization of data and the growing usage of internet, cyber attacks pose a real threat to organizations of any size. Numerous major data leaks from otherwise reputable websites or platforms are frequently reported, with millions of private information including email addresses, passwords or bank account details, being distributed publicly. On January 2019, the biggest collection of leaked data, called Collection #1, was distributed in the dark web for free, followed by Collections #2-5. These huge datasets consist of roughly 2.7 billion email and password entries from over 2000 databases and include leaked information not only from older data breaches, but also new ones [1]. Other big incidents include data leaks from MySpace with 427 million accounts [2], LinkedIn with 164 million accounts [3], and 64 million Dropbox accounts [4].

Many of these malicious cyber attacks happen by exploiting some existing known or unknown software vulnerabilities. However, this is not always the case; sometimes the attacks are successful because of human negligence. In fact, people play a significant role in data security, whether they are working as computer scientists or if they are simply using a computer for their daily job. Lineberry had identified the human element to be "the weakest link" in security, back in 2007 [5]. This has not changed much over the years; it has been reported that the human error or negligence was the reason for 27% of data breaches during 2018 [6]. Another survey in the same report shows that phishing accounts for 67% of the cases of an unintentional security compromise while weak or reused password are responsible for 56% of them [6].

It is, therefore, essential for any organization to have a well-established set of security rules and ensure that it is followed by its employees. However, Cisco reports that the lack of untrained employees is yet one of the greatest obstacles to security, with a growing tendency over the years of 2015 to 2017 [7]. It is evident that cybersecurity awareness training in organizations has become more of a necessity than a choice. Investments done by organizations in personnel training have been increased to 42% in 2017, up from 38% in 2016 [7], in order to minimize the potential data loss due to security breaches. It is essential that everyone who interacts with computers on a daily basis needs to be aware of the possible threats and their consequences.

Personnel training on cybersecurity awareness can be achieved through multiple ways, which can either substitute or complement each other. More specifically, serious games can be used to make training programmes more appealing towards the employees and consequently aim for higher learning effectiveness [8]. The term "serious game" is used to signify games that have another primary objective than pure entertainment, such as to educate, train or create awareness. In the past, serious games have been used for teaching cybersecurity, most notably for government sectors, such as the US Airforce [9], the US health department [10] or the US Navy [11] through their Naval Postgraduate School, but also for using them as alternative methods of education, in order to familiarize younger audiences with the threats of cybersecurity and teach them how to defend themselves against them [12] [13].

This master's thesis aims to enrich the academic knowledge gap which exists in teaching cybersecurity through serious games in a working environment, by presenting and studying the two games *Surf Clean* and *Cyberzen Desk* which were developed by Manzalab Group and published by Cyberzen. During the writing of this thesis, I was initially an intern and later employed by Manzalab Group, which gave me the opportunity to study and present the two games whose purpose is to teach cybersecurity principles. Both serious games that will be presented in this paper have been commercially used by several organizations, most

notably two large French banks, a police department and a private insurance company in the context of cybersecurity awareness training which were held up by each organization.

Additionally, seeing that there are not many publicly available academic papers that examine commercial off-the-shelf serious games, this thesis will manage to fill certain knowledge gaps that exist there. The purpose of presenting these two games is to propose two different serious game designs, in order to closely examine them and analyze the cybersecurity concepts that they try to convey to their audience. At the same time, we can review their effectiveness as serious games from a pedagogical point of view but also their acceptance from the audience who played them as part of their cybersecurity awareness training programme.

Below there is an outline of the thesis structure:

- The first chapter introduces the reader into the concept of this master's thesis and presents its research questions as well as the motivation behind the chosen topic.
- The second chapter focuses on the background topics on which this thesis is built upon; the two main points of interest are cybersecurity with an emphasis on the human element, and serious games.
- On the third chapter, the two games are described, both from a pedagogical point of view and from a game design aspect. Initially *Surf Clean* is presented, going in depth on the three scenarios that comprise this serious game, with a focus on the storyline and on the topics it covers. The second part of this chapter describes the game *Cyberzen Desk*, with its setting overview and the objectives of the player.
- The fourth chapter shows the results of a player satisfaction survey that was conducted on one of the companies who used the serious game *Cyberzen Desk* as part of their employee awareness training.

- The fifth chapter discusses the findings from the user feedback that were presented in chapter four, but also evaluates the game *Surf Clean* from an educational point of view, with an emphasis of what can be improved to maximize the user learning effectiveness.
- Finally, chapter six presents the conclusions for this master's thesis followed by suggestions for future research on this topic.

2 Background

This chapter gives an overview of the topics that are related to this master's thesis. Initially, the chapter starts by presenting the topics of cybersecurity and cyber attacks, while emphasizing on those attacks that are targeting to exploit human weaknesses. It then transitions on the countermeasures that are needed to be taken against this menace: we focus on employee training on cybersecurity. Many important factors are explored, and serious games are presented as an attempt to overcome certain issues that have been observed to be the reason behind diminished learning outcome. Lastly, some related work is presented with some successful projects which used serious games for cybersecurity training and education.

2.1 Cybersecurity

Cybersecurity refers to the protection and prevention of damage to computer systems, networks and software, together with the information and data held in them, which can be caused by digital attacks [14]. The preservation of the data that are contained in the aforementioned systems, is commonly known as information security and it is an integral part of cybersecurity. The objectives of both cybersecurity and information security are based on three fundamental principles: maintaining the confidentiality, the integrity and the availability of the data [15].

To begin with, confidentiality can be described as the protection of sensitive information within an organization. This includes the assets and secrets of the organization as well as the personal data of their employees and clients. Moreover, the principle of data integrity refers to the ability of ensuring that the data has not been tampered with without proper authorization. This includes modifying or deleting existing data with the intention of causing harm. Finally, the concept of availability refers to the ability of maintaining the data and the network systems always accessible if possible, or otherwise certifying a quick restore of the systems in case of an unexpected downtime. This could be the result of a sudden power loss or a system failure, but other times it could be coming from an external attacker, trying to disrupt the systems by executing a Denial of Service (DoS) attack [16].

2.2 The Human Element in Information Security

There are multiple elements that can help strengthen the security defenses against cyber attacks. Unfortunately, the same elements that can be used to strengthen the defenses can also have the opposite effect, if not applied correctly. More specifically, cybersecurity can be viewed and analyzed from two different aspects: the technical and the social one [17].

The technical aspect of security includes following the security principals when designing and creating a new web application, software or database. For example, during the development of a web application, one can refer to the "Open Web Application Security Project (OWASP) Top 10" to understand and avoid making the most crucial security mistakes [18]. In addition, multiple types of technical measures can be taken to ensure the effective defense against cyber attacks, such as proper installation of firewalls in the network of an organization and antivirus software on personal devices.

On the other hand, the social part of security is solely represented by the people and consequently, their actions. Different types of individuals can be observed within an

organization, ranging from executive and managers to end users and production workforce. Altogether, the behavior of the people of an organization can be described collectively as "organizational culture". However, the unpredictable nature of humans poses a great challenge for managing cybersecurity threats that are related to people. Evidently, the individual personality and behavior of every person does not always align with the one of the organizational culture's norm [19].

Cybersecurity threats can be distinguished into adversarial and non-adversarial. The adversarial threats stem from those that want to deliberately cause harm to the organization, such as enemy organizations, individuals or other types of opposing groups. On the contrary, non-adversarial threats suggest that they are the result of an unpredictable event such as a natural disaster, or a human error that was made unintentionally [20]. The point of view of this thesis is towards the adversarial threats that are looking to exploit human weaknesses in order to successfully execute a cyber attack.

2.3 Cyber attacks and the Human Element

According to the ISO/IEC 27000 a cyber attack is "an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset, which is anything that has value to the organization" [21]. In the case of an attack, security experts try to understand the impact that that attack has had on the organization by analyzing the means that lead to the success of the attack. The data extracted from the analysis can be used to provide invaluable information of existing vulnerabilities and help the design of countermeasures and possibly new security policies.

In order to address the complexity and multi-dimensionality of today's attacks, Kjaerland [22] presented a taxonomy of cyber attacks, which was later refined by Simmons et al. [23]. In the given classification, they identify cases where people are the main actors in an attack,

directly or indirectly, such as misuse of resources, social engineering, installed malware and phishing attacks.

2.3.1 Misuse of resources

A misuse of resources implicates the unauthorized use of information systems [22] by an employee of the organization, while often exploiting their access privileges [23]. The motivation behind these types of acts can vary, as well as their severity. For instance, sending or receiving emails on the professional account which are out of the work context, may lead to legal or financial risk. In more dangerous cases, an employee might use their authorization levels to gain access and possibly modify the organization's data [24] with the intention of using them or selling them to an adversary. Moreover, an employee could use social engineering to fool a colleague into providing them access to information that is outside of their clearance level.

2.3.2 Social Engineering

Social engineering has been defined as the use of social disguises, cultural ploys and psychological tricks in order to manipulate a person into helping an attacker with their intrusion plan or to gain access on the computer systems and networks [25]. In reality, social engineering is a type of attack, where the social engineer is trying to exploit human weaknesses in the same way that a hacker is trying to exploit a system's vulnerabilities. The attacker will often try to influence their victim's emotions by creating feelings of fear or excitement, or other times will try to develop confidence and trust [26].

The attacker will present a false but believable story to their listener and will try to create a state where they find themselves trapped and need the victim's help to escape. With a lot of manipulation tricks, they will try to avoid answering certain security questions with an

ultimate goal of gaining any information they need in order to continue with their attack plan. Other times, social engineering is the reason why people accidentally install malware and expose the organization's network, as we will see later on. Due to the exponential growth of social engineering occurrences over the past years [27], it is without a doubt a great enemy to an organizations' information security.

2.3.3 Malware

A malware is a piece of software with malicious intentions that will try to act without the permission of the user, in order to compromise the confidentiality, integrity or availability of the information system [28]. While malware itself is essentially comprised solely by malicious code and it therefore seems to belong in the technical aspect of security and malware detection, it also relies on human actions to initialize its malign operations. It is therefore essential to closely examine the various types of malware and identify how human actions can facilitate, allow or prevent an attack. Based on its behavior, a malware can be classified into the following categories.

Virus: A computer virus is a malicious software that attaches itself onto other executable programs, or files such as images or PDF files. The infected program or file will spread to other programs or files, as soon as it is opened or executed and thus the infection can grow exponentially. A sophisticated virus, might try to hide its existence using techniques such as mutating itself or changing its signature [29] which makes them a very dangerous enemy, since they can exist undetected for a long time.

Worm: On the contrary, worms can act independently without the need of attaching to an existing piece of software or file. They have the ability to spread within a network and take advantage of any existing vulnerabilities [29]. The activation time for each worm can range from instant to days. This is due to their activation mechanism; it can be either scheduled or

human activated. More specifically, the worms that are relying on human actions to be activated, often use persuading techniques to convince people to execute them [30]. These social engineering techniques provide false and misleading information to the user in order to achieve their purpose and manage to reproduce.

Trojan: Trojans have acquired this name to signify the hidden threat that they carry. This This type of malware once it is launched, will establish a connection to a remote location which grants many possibilities to the attacker. For instance, the attacker can access the infected system and install other malicious programs, can read personal or professional files and emails [29] but also disable firewalls and antivirus programs to conceal their existence [31].

Ransomware: It is usually in the form of a Trojan [31], but it has also appeared in the form of a worm in the case of WannaCry ransomware attack [32]. This type of malware will encrypt the user's local files, such as important documents and images. There may be occasions that the ransomware manages to access files through the network accessed by the infected computer and lock those files as well. Unlike the types of malware presented above which try to act quietly and stay undetected for as long as possible, a ransomware will quickly reveal itself to the user, showing a message which explains the situation and requests for an amount of money in exchange for the files [31], usually through bitcoin or some other cryptocurrency. During May 2017, WannaCry had an enormous outbreak, infecting over 150 countries with a paralyzing impact on multiple sectors including health, industry, education and telecommunications [32].

2.3.4 Phishing attacks

Phishing is a social engineering technique, by which a perpetrator seeks to obtain sensitive data through a falsified email or web site, on the pretext that they are representing a legitimate

business or a trustworthy person [33]. For example, a phishing attempt could be through an email, where the sender uses the name and the logo of a reputable bank in order to convince the recipient that they are an actual associate of the bank. After gaining their trust, the email may prompt the receiver to click on a fraudulent link which will probably lead to a form to fill out with personal information such as name, password or bank account details. However, this is only one of the possible attack scenarios.

Over the years, different types of phishing techniques have been observed, and they are evidently becoming smarter and trickier to detect [34]. As seen through the phishing taxonomy that was proposed by Aleroud and Zhou [35] (Figure 2.1), the attack techniques can be organized in three main categories: attack initialization, data collection and system penetration. Attack initialization is often related to social engineering [36], where the phisher will try to manipulate the end user into thinking that what is presented to them is real. After the user has been finally tricked that they are looking at a legitimate website or email, the phisher passes onto the data collection of the user which can be achieved through different ways, such as fake web forms or keyloggers [35]. Lastly, system penetration techniques such as fast-flux and cross site scripting can be used to ease the attack initialization or other types of cyberattacks [35].

Phishers' primary goal is to present to the end user a believable content. What defines a "believable" content though? As seen through literature, there are numerous factors that govern a user's decisions when it comes to detecting a deceiving content.

To begin with, the human lack of knowledge of computer systems and applications poses a great enemy against cybersecurity, because it can be largely exploited by phishers [37]. For instance, many people fail to interpret security indicators such as SSL. Even though it has been reported that people have slightly better security awareness over the years, there is

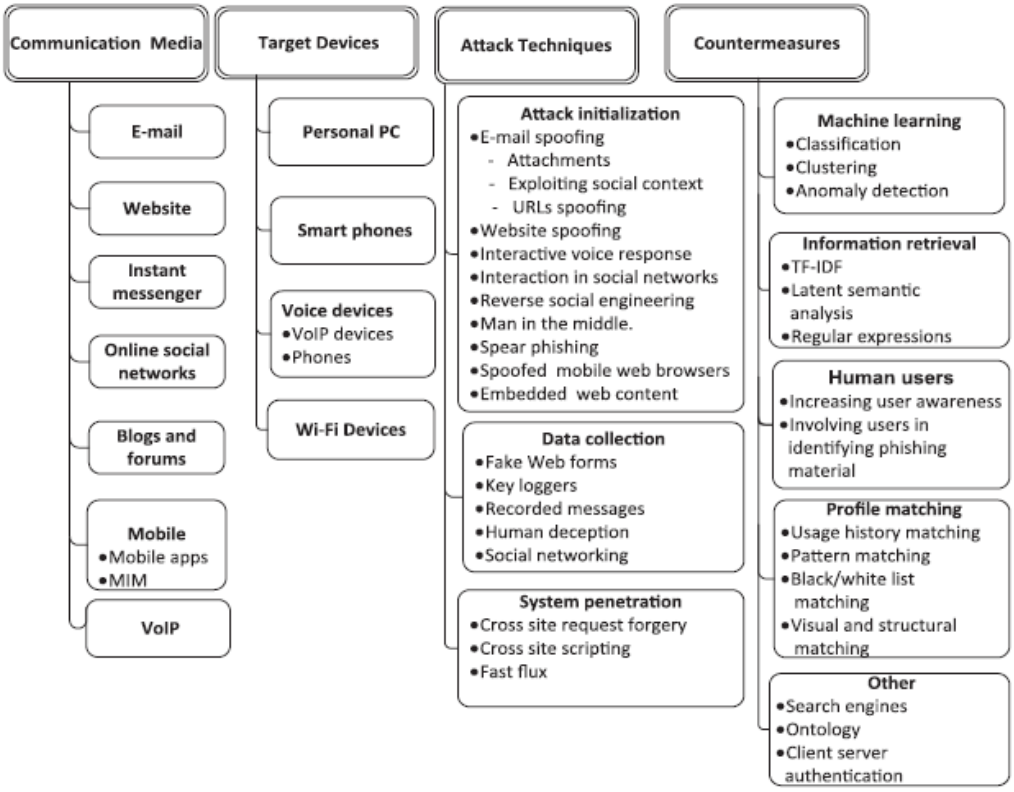

Figure 2.1: Phishing attack taxonomy (Source: Aleroud and Zhou [34])

still a large portion of people who do not find that browser indications can eventually help them to correctly identify a phishing trap [37] [38].

According to a study that was using eye tracking analysis to capture the participants' interactions with the computer, they only spent 6% of the time looking at the browser's chrome for any security hints, such as the existence of the SSL padlock [38]. Participants in another study said that the existence of the padlock within a webpage is more crucial than its existence on the chrome of a browser [37]. Therefore, it is easy to assume that people do not have the appropriate knowledge or do not pay the attention needed, concerning the security indicators on a browser.

Another common tactic that phishers use is having a bad domain name, usually one that closely resembles the original website name. For instance, if a bank holds the domain of `www.bankname.com`, then a phishing website could have names such as `www.bank-name.com`, or `www.onlinebankname.com` [39].This could easily elude someone who is not aware of the exact official bank URL or does not even suspect a phishing attempt. Alternatively, a domain name might have been "typejacked" by substituting the original letters with others that look very similar, as in the case of using 1 (number one) instead of l (letter "L") [37] or using Unicode characters that do not belong in ASCII by exploiting a browser vulnerability [40]. Moreover, many people ignore the fact that an email header can be manipulated to show in the "From" field any email address a phisher wants, in order to mislead the recipient regarding the actual sender [37] [41] [34].

To make matters worse, through URL spoofing a phisher will try to disguise a fraudulent website to look as if it is genuine, by manipulating its URL address or the address bar of a browser. Spoofing can be carried out in various ways. Notably, a phisher can use JavaScript to obfuscate the address bar of the browser so that the URL will look legitimate, when in fact it is not. In addition, with the aid of JavaScript the phisher can also spoof the "https" and the lock icon that signifies that a page is secure and certified. Such manipulation can be achieved through the usage of embedded JavaScript directly on a phishing website, or by redirecting a user from the official website that he or she tries to visit, to the phishing one because of some installed malware [36].

Another way of stealing personal data is through pop-ups that ask for user credentials. Numerous times a malicious website, or even an infected legitimate one might prompt a user to enter their credentials in order to continue using the website. In the study that was mentioned earlier, 62% of the participants failed to realize that the pop-up had the wrong URL address, even though they spent an adequate time investigating it [38].

On more recent news, a very deceptive phishing campaign was discovered involving login pop-up windows [42]. In this case, it was reported that the phishers would exploit the frequent occasion where a website will prompt the user to sign in using their Facebook account, to avoid the hassle of creating a new account. The fake Facebook login form pop-up that would be shown, would be an exact replicate of a legitimate one, including the URL, the SSL padlock and HTTPS. However, in reality it is not a real pop-up that actually redirects to Facebook, but rather a pop-up that was created by HTML and JavaScript. Therefore, the only way of realizing if it is actually a false pop-up is for the user to try and drag the popup outside of its window; if it gets hidden as it exits the browser window, it means that it is not a legitimate pop-up window.

Furthermore, a phishing attempt can become even more credible when its content is really tailored to one's personal interests. Social networks can be particularly helpful for hackers to successfully deliver their attacks, due to the amount of information that can be obtained from a social network profile concerning contacts, interests or community groups [34]. This is often the case when an attack is targeting a specific organization, which is called a spear-phishing attack.

Spear-phishing attacks have some explicit goal which is usually concerning stealing valuable information or compromising security [43]. By cross-referencing information on employees found in professional social networks such as LinkedIn with their personal ones such as Facebook and Twitter, one can collect a great deal of personal and professional data. Afterwards, a phisher can use this mined user data to syntax the ideal email, with a tempting title and a content that reflects the personality of the target, or one with professional content, related to their current work. To make things worse, the phisher can sign the email as a familiar name by picking one from the victims' contacts either by creating an email address with their name or by spoofing the email address with the technique mentioned earlier [43].

To sum up, it is evident that phishing attacks are targeting to exploit human weaknesses with various ways. Depending on the strategy that a phisher has, it can become very challenging to discern some phishing content, due to lack of knowledge, distracted attention or sometimes because of sophisticated concealing methods used by the phisher. Even when people are expecting to face a fraudulent website, the success rate in correctly identifying it is really low, according to a recent study [38]. Nevertheless, it is apparent from the literature [43] but also from the security experts' advice [44] that the education of an organization's personnel should always be a very high priority, no matter the size or goal the organization.

2.4 Hacking and Social Engineering Motives

To have a better understanding of the threat that a social engineer or a hacker poses to an organization, it is important to visit the motives behind a social engineering or cyber attack. A person who uses social engineering for malicious purposes, closely resembles a hacker in motivations, aspirations and expectations. Similarly to a hacker's motives [45], a social engineer can have various reasons for attacking a person or organization. One may have a single motive or multiple ones when carrying out an attack.

2.4.1.1 Monetary Gain

Some attackers have as a motive the financial compensation that they receive from the attack. Depending on the type of the attack, the money can come through fraudulent money transfers, credit card theft, stealing and selling valuable data, extortion, fraud [45], identity theft and more. However, this is not the only way that a hacker can get a compensation. A more indirect way of gaining money out of hacking is by offering "hacking as a service". In short, this term refers to the people who will offer their hacking skills accompanied by state-of-the-art tools, to anyone who wishes to hire them for a great amount of money [46].

2.4.1.2 Intellectual challenge and peer recognition

In other cases, the incentive of a hacker is to face a challenge and succeed [45]. Although this does not necessarily mean that the person is doing it for peer recognition and appraisal, it has been shown that social factors are correlated with the frequency that one engages into hacking activities [47]. From the numerous hacker forums that one can discover browsing on the Internet, we can conclude that there is a tight community of people who exchange experiences and ideas related to hacking activities [45] [46]. In order to be accepted and respected in these communities, one may be asked to demonstrate their skills as well as possibly share hacking tools they have created [45].

2.4.1.3 Hacktivism

Hacktivism is a term deriving from the words hacking and activism. While activist acts use traditional demonstrations and protests as a means to achieve a purpose, hacktivism uses the Internet. However, the hacktivist collectives draw the line between right and wrong at their own judgment. It therefore depends on the actual hacktivism actions to determine if an act is criminal or not. The motives of a hacktivist are usually related to their perceived image of injustice towards social and political dimensions [48]. Thus, some hacktivist actions may seem more like a nuisance or embarrassment to the attacked party [48], whereas others can take more serious extents [49]. Moreover, those attacks are by definition targeted attacks, usually towards some business company, political party or governmental institution.

2.5 Security Training and Awareness

Every organization regardless of its size, needs to have a well-defined security policy. A security policy is a collection of directives, regulations and rules that dictate the way that an organization manages, protects and distributes information [50]. In other words, a security

policy defines the user actions that are allowed and the actions that are disallowed [51] in order to ensure the preservation of the confidentiality, integrity and availability of data, as they were described in the beginning of this chapter. In order to have an efficient security policy in place, an extensive risk analysis needs to be performed by security experts in order to identify the threats to the organization, the system's weaknesses as well as the assets that are most valuable to the organization.

While some ground rules might be the same for most organizations, such as the enforcement of having some antivirus software installed on every work computer, other rules can differ from one organization to another. This is due to the fact that each organization has different priorities on what they consider valuable data, which is usually related to their main activity. The security policy of the organization needs to be communicated to their employees and it is expected from them to adhere to its rules. However, as it was mentioned earlier, people's habits and behavior often deviate from the cultural norm that an organization has [19] and consequently affects their compliance to the existing security policies [52].

Employee compliance can be significantly improved by threat appraisal [52] through various educational ways. It is therefore essential that employees understand the reasons why following security policies is crucial. For instance, employees need to be aware about the advantages of using some antivirus software. People often find themselves frustrated by the installed antivirus, for various reasons.

Common reasons include but not limited to mistakenly deleting or moving to quarantine an important file or executable or taking up significant computer resources. Both may result in delaying their overall production process, and in situations like these, one may be tempted to disable their antivirus temporarily or permanently. As a result, this might end up compromising their device and consequently put in danger the internal network of the entire

organization. An employee informed about the dangers of such an action, is less prone to making such a reckless decision.

Other ways that are being used to motivate employees to follow the security policies of the organization, are by sanctioning or rewarding a behavior [8]. However, scholars' findings on these topics are not aligned regarding the sanctions or intangible rewarding correlation with user intention to comply with the policies [52] [53]. Another research suggests that this is probably because there was no immediate connection between the rewarding system and the adherence to the security policy [54].

In the end, user awareness and education seems to be the most reliable way of transmitting the appropriate knowledge to the employees [52] concerning what information security policies are and why it is in the best interest of everyone they are being followed [55]. As it has been discussed earlier, lack of user knowledge can lead to great vulnerabilities. As an example, a typical but serious user mistake is the choice of a weak password. This could occur both in a professional account within a known platform or website, but also in administrator passwords in the internal company network and servers. In literature [56] it is observed a high tendency of employees choosing very weak passwords that can be broken in less than one minute. However, after a one-year security awareness programme dedicated in selecting a strong password, there was a noteworthy improvement amongst the employees.

2.5.1 Increasing Training's Effectiveness

Applying a security awareness project to a company cannot always guarantee a successful outcome. There are, nevertheless, some guidelines to be followed in order to facilitate the learning process and overcome some common mistakes.

To begin with, educational programmes should to be tailored to the needs and organizational culture of each business. Before designing a programme, one must first clearly define the learning objectives; what are the security points that the training session will be focusing on? While introducing some base rules such as choosing a strong password can be useful to everyone, there are always some security guidelines that are specific for each organization [8]. Moreover, conducting security audits or questionnaires to the personnel of the organization in question before designing the training programme, can provide invaluable information concerning their weakest points and their initial threat awareness.

After having the clear learning outcomes defined, another point needs to be addressed: how can the learning content be attractive to the trainees in order to captivate their attention and therefore succeed in transmitting the necessary knowledge? It is therefore important that programmes are designed in mutual collaboration of security experts and User Experience (UX) designers. The security experts will guarantee that the information that is given is accurate and useful for achieving the pedagogical objectives that were defined in the beginning. At the same time, a UX designer who is a professional in ensuring that the end content which is presented to a person is user-friendly and intuitive, and thus facilitate the learning process by making the security training programme attractive to them. In addition, it has been noticed that a more realistic training environment can aid the user's learning outcome [8].

Literature strongly recommends that the materials which will be used to train the employees should avoid being too technical, so as to be understandable by everyone [19, 8]. Otherwise, the people who are struggling with understanding the security terms and the reasons why the policies should be followed, might eventually be demotivated to apply the given guidelines [55]. It is also advised that the training should be engaging and maybe in the form of a short movie or animation, since lengthy texts in the form of reports or articles can result in being perceived as a "burden" [56]. Other experts seem to agree with this alternative way of

teaching, suggesting that real-world examples through immersive programmes can lead into a successful staff training concerning cybersecurity threats and security policies [57].

In the end of the training or awareness programme, if the initial employee evaluation is paired with a follow-up evaluation, it can provide concrete information on its overall effectiveness. The areas with the biggest improvement can be identified and considered a successful approach. On the contrary, the areas where the employees have shown the least improvement can be examined closer, either to redesign the existing pedagogical approach or create new educational projects that will be focusing onto the weakest fields. In fact, it has been emphasized that security awareness trainings should not be a one-time procedure, because people tend to return to their old, non-secure habits after a while [57] [8].

2.6 Serious Games

Previously we reviewed some common pitfalls of educational programmes and discussed about what should be done differently to increase the overall effectiveness of the cybersecurity training programme within organizations. While traditional education may struggle with such issues, serious games can be used instead to overcome those limitations.

Initially we should start by defining the notion of a “game”: according to the literature [58], a game is mainly consisting of three basic elements: the players that take part in the game, the rules that define the game’s limitations and finally the goals which can incentivize the players to play, to form alliances with other players or to create rivalry between them. Both physical and digital games aim to entertain their players with their content and design. Even though teaching is not one of the primary objectives of a game, it has been argued that games can result into a player learning new things, as a secondary effect [59] [60].

Nevertheless, there are games that may seek to have a primary purpose other than pure entertainment or fun, as defined by the scholars [61] [62]: they are called Serious Games. Corti has extended the definition by adding that serious games *"is all about leveraging the power of computer games to captivate and engage end users for a specific purpose, such as to develop new knowledge and skills"* [63]. A serious game can have different primary objectives, depending on their target market: we can therefore find Military Games, Government Games, Educational Games, Corporate Games, Healthcare Games, Political Games, Religious Games and Art Games, as defined by Michael and Chen [62]. However, as pointed out by other researchers, this market-based way of classification can be easily outdated, due to the constant expanding of serious games [64].

In agreement with the G/P/S model proposed by Djaouti et al., serious games can be classified based on Gameplay, Purpose and Scope. While the gameplay includes elements such as the rules and the universe of the game and the scope is broader sense of the market-based classification, the purpose provides another way of classifying serious games: message broadcasting (educative, informative, persuasive or subjective), training (cognitive or physical) and data exchange [64]. From another point of view, Laamarti et al. see serious games as *"an application with three components: experience, entertainment, and multimedia",* and compare them with other activities such as computer games, training simulations and sport games, as seen in Figure 2.2 [65].

Following the numerous definitions of serious games that can be found in the literature, many design frameworks have been proposed as well. The purpose of a design framework is to provide the guidelines for the creation of a serious game, in order to increase its learning effectiveness [66].

A recent study by Tsita and Satratzemi [66] that has reviewed some of the most known frameworks [67] [68] [69] [70] [71], proposed four conceptual divisions to classify their

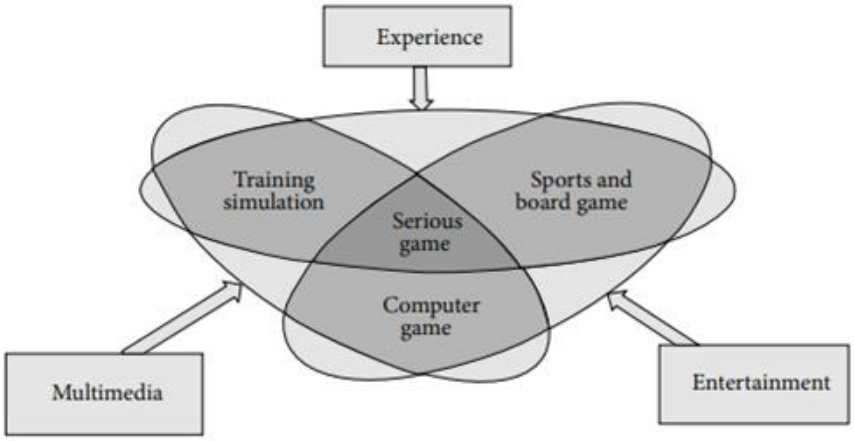

Figure 2.2: The three components of Serious Games. (Source: Laamarti et al. [65])

characteristics: the learners' specifications which refer to the target audience of the serious game, the learning intentions concerning the teaching objectives, the game attributes that precise the gameplay and interface experience, and finally how to facilitate learning for the end user [66].

The study's overview of the specifications of a serious game aligns with the guidelines which were identified in the previous section concerning increasing the effectiveness of security education. Defining the learner's specifications corresponds to identifying the culture of an organization and designing the security education programme according to the employees' needs and weaknesses refers to the teaching objectives. In the game attributes section multiple similarities are observed; a carefully designed User Interface (UI), which is the means that a user can interact with the game, can be significant in improving User Experience (UX). Moreover, rewarding an exceptional employee behavior in terms of following the security policies could correspond to the in-game rewarding: score points, earning badges or simply a verbal praise that will give the player a sense of self-accomplishment.

Lastly, looking at the ways to facilitate learning it is observed that many frameworks highlight the importance of the psychological flow state. The flow state refers to drawing enjoyment from an activity with defined goals while being immersed in it, but also managing to pay attention to what is happening, as defined by Csikszentmihalyi [72]. Aiming to achieve such a state in a serious game could help overcome the shortcomings that were mentioned earlier concerning outdated text-based security education programmes.

By extension, the challenge of the training material often being too technical can also be tackled through serious games, as scholars suggest that having an escalation of content difficulty throughout the gameplay experience can captivate the player's interest since it will be evolving based on their current skillset, which follows the principle of the flow [68]. Another interesting conclusion of that study was that almost all the examined frameworks provide immediate feedback as a mechanism to facilitate the end user's learning process [66]. This is a clear limitation in more traditional teaching or training methods in which feedback is often delivered with delay, for example at the end of a quiz.

2.7 Related Work

Over the years, serious games have been developed and used to teach cybersecurity principles to several kinds of audiences. Gestwicki and Strumbaugh [60] present a three-tier model of classifying games based on their gameplay and their learning objectives. The first type includes those games that have an abstract mention of cybersecurity, through linear narration and/or their general theme. Even though these types of games could be useful as an introduction to cybersecurity for younger audiences, they do not carry significant learning potential. In fact, the concepts of cybersecurity that are presented in such simplicity might result in misleading beliefs of what cybersecurity is or what kinds of threats exist.

The games that are in the second tier are less linear: their stories and outcomes change based on the choices of the player. However, even if the user is called to make a choice in the moment, their choices are still predefined, and the possible outcomes are all predictable. Nevertheless, they can be utilized to teach some cybersecurity concepts throughout a storyline and the user results can be reviewed to understand the level of the user's understanding of those concepts.

A serious game that fits this tier is *Cybersecure* by HealthIT.gov [73] which presents realistic situations that someone who works with patient health records may encounter. In these situations, the player is presented with some options and gets rewarded with score points and office upgrades for answering correctly. The game teaches cybersecurity fundamentals from password management to the importance of correct storekeeping and handling of private data. However, the narrative is not following a consistent storyline but rather presents independent case-scenarios followed by a specific dilemma. This lack of flow may eventually wear the player out, as the immersion might slowly fade after playing this game for a brief duration of time. On the other hand, presenting simple and independent scenarios can potentially be beneficial to the player to help them have a clear idea why this situation is crucial and consequently what the current learning and gaming goal is.

Lastly, the tier-three games are more sophisticated, as they require more critical thinking from the user to be able to analyze a situation and make a decision that is not predefined or proposed. The authors mention that the games that are classified in this category are closer to the meaning of a "game" as they are more competitive, but also because the freedom of choice and decision making are more evident throughout the gameplay.

For this tier, we can take as an example the game *Cybersecurity Lab* by NOVA Labs [12] which aims to teach younger audiences basic but important topics on cybersecurity and

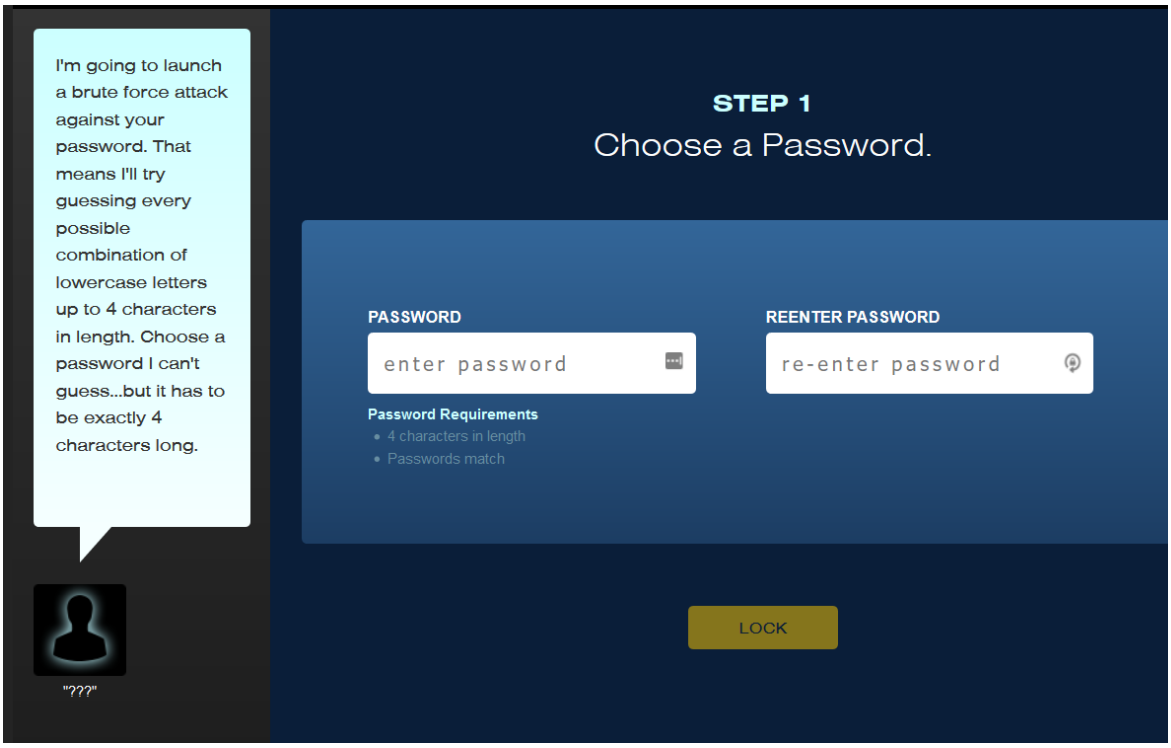

Figure 2.3: Choosing a password training: the player can observe the consequences of choosing a weak password. (Source: Cybersecurity Lab by NOVA Labs [12])

computer science. The game has three different types of minigames, each focusing on teaching three essential notions:

- *Choosing a strong password:* the player is given the task to choose a password with certain requirements(Figure 2.3). For every next level, the requirements grow, and consequently the passwords become more secure. Brute force attacks and later dictionary attacks are also introduced to the player: the player's password as well as the opponent's are being tested with those attack methods, with an option of adding later on more parameters: symbols, numbers, capital case letters
- *Introduction to programming:* the player is introduced to some basic concepts of programming: commands, conditions and loops, which help the growth of logical thinking. The environment is child friendly and does not require from the player to

type any code: the code parts pre-exist in the form of puzzle pieces and the user can drag and drop them to create the programming blocks, depending on what the objective of the exercise is.

- *Identifying phishing attacks:* for this task, the player must identify the clues of potential phishing attempt on the text, image or audio that is presented to them. For each phishing case presented and after the user has completed the challenge, additional information is given to the player that explains why certain things should be red flags for anyone who encounters them.

Cybersecurity Lab is designed very carefully in order to manage to keep the player's interest and does so by slowly increasing the difficulty of each topic, while explaining what the best practices are. What is also worth mentioning is that the game initially pushes the player to make a bad choice concerning choosing a password, only to strongly emphasize the problem that it poses and present the player into the notion of brute force attack (Figure 2.3).

Continuing with the overview of other serious games for cybersecurity, *CyberNEXS*, developed by Science Applications International Corporation (SAIC) aims to teach more advanced topics in cybersecurity. It is a type three game on the three-tier model presented by Gestwicki and Stumbaugh, which is confirmed by the strong element of competition found in the gameplay [8]. Through this game, one can expect to develop several skills such as identifying and mitigating cyber attacks, cyber forensics after an attack has taken place, penetration testing and a Capture The Flag (CTF) mode in which the players attempt to take over the other team's network system by exploiting vulnerabilities, while at the same time defend the incoming attacks at the network that they have taken over [8] [74]. It has been used both by high school students but also by professionals who want to simulate real-life situations [74]. However, a more profound understanding of cybersecurity topics is needed before playing this game.

Moreover, the serious game *CyberCIEGE* which was developed by the US Naval Postgraduate School (NPS) is a management game in which the player is called to make decisions and allocate their financial resources how they want, in order to ensure the security of their networks. The concept is similar to the one of *SimCity* by Electronic Arts (EA) [11], but instead, the player will spend their budget on employee security training, new workstations, upgrading servers and other similar actions, in order to ensure that the security policies are followed and all the company's assets are secured [75]. The game's aspiration is that the player will be actively learning and experimenting during gameplay, while maintaining the "flow" [76]. Furthermore, *CyberCIEGE* is a project that has been evolving for at least ten years with its creators constantly adding new content, and has been used by educators all over the world most notable in the sections of military, defense and secondary or tertiary education [76].

A more recent project, *GenCyber* by the National Security Agency and National Science Foundation (NSA/NSF) [77] includes four games which aim to teach four different concepts of cybersecurity to high school students, but also to generally motivate minority students to pursue a career in cybersecurity in the future. Each game has a different didactical objective:

- *Social engineering and information security game:* it simulates an office environment which the player can experience through 3D VR, where people will attempt certain behaviors that try to exploit human weaknesses, such as Piggybacking. Piggybacking refers to the act of taking advantage someone's access rights to enter a restricted area, by physically walking right behind them. Those types of scamming behaviors can be experienced through this game, in order to raise awareness and prevent such from happening in reality.
- *Secure online behavior game:* this game trains the players to identify phishing attempts in written or oral form. The game is also in a 3D VR world, within familiar environments for the students: the school's computer lab or in front of their personal computer.

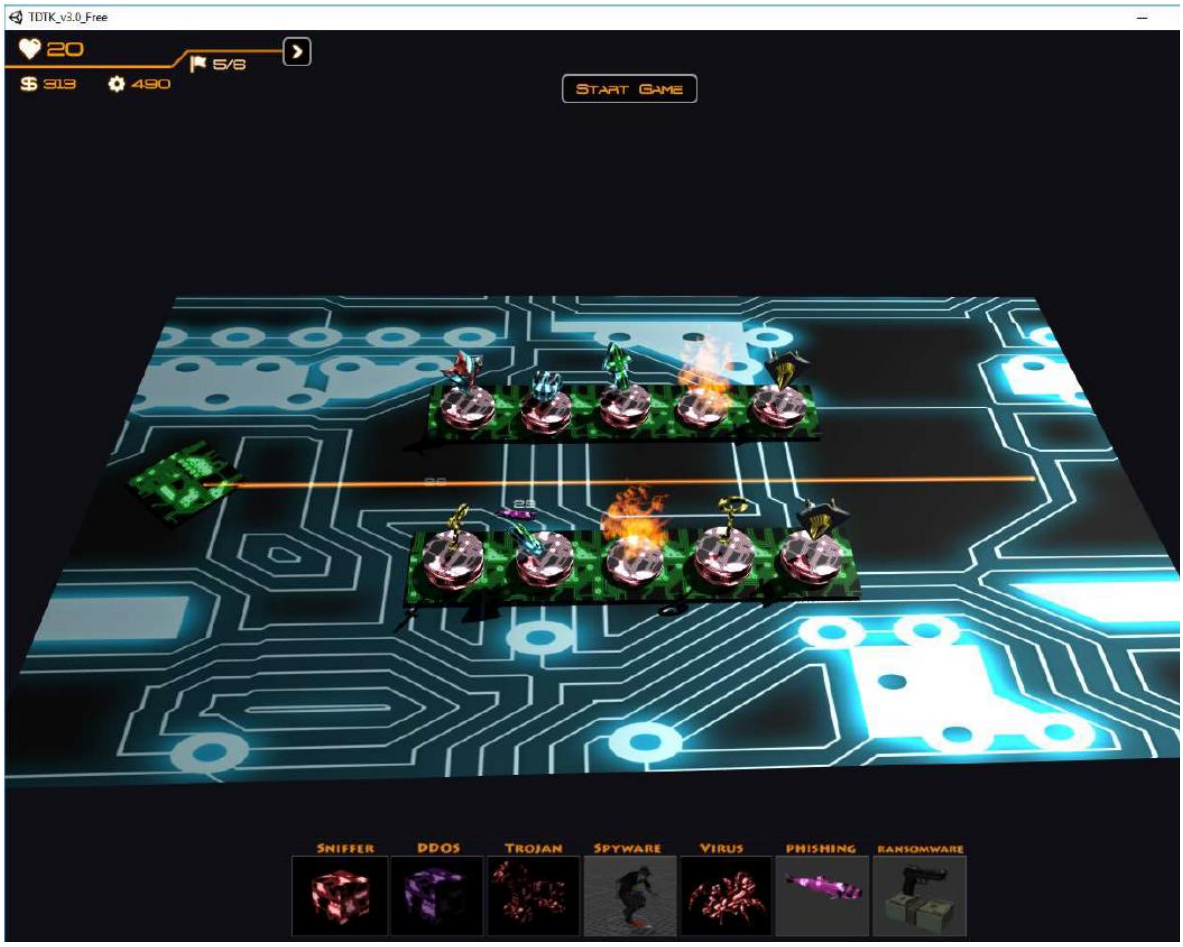

Figure 2.4: Cyber tower defense game by GenCyber game (Source: Jin et al. [77])

- *Cyber tower defense game:* the player is expected to act quickly by choosing the appropriate type of defense in order to stop the incoming cyber attacks, and secure their network and servers (Figure 2.4).
- *2D GenCyber card game:* the game can be either played in physical form with two players, or digitally, by one player against the computer. The card game is a knowledge game which includes questions from different topics in cybersecurity and networks [13].

Researching through the literature, several serious games aiming to teach cybersecurity concepts were found. Some of them are targeting school students, such as *CyberAware* [78] which is addressed to young children starting at 6 years old and aims to raise awareness for matters such as malware, cyber attacks and spam, while others can be played by more mature audiences, such as *Anti-Phishing Phil* [79] whose objective is to make people aware of phishing scams.

Another interesting point that is made through the paper by Gestwicki and Stumbaugh [60] is the identification of certain games which were not developed as serious games, yet they achieve to have a pedagogical outcome on certain cybersecurity principles. For instance, in the game *Deus Ex: Human Revolution* by Eidos Montreal there is a minigame where the player is required make quick, strategic decisions to hack a network topology in order to grant themselves access to a computer terminal ora sealed door.

Overall, cybersecurity training has been constantly challenging past literature as new technologies are being developed which make an impact on the research done. It is therefore, strongly suggested for future researchers to take into consideration such changes as to identify clear patterns and trends without leaving major aspects unnoticed, which could sometimes be hidden, as with the case of the aforementioned game *Deus Ex: Human Revolution.*

3 Serious Games for Cybersecurity

For the purposes of this master's thesis, the company Cyberzen provided two serious games for presentation and analysis:

- *Surf Clean*: a serious game about social engineering and fundamentals on cybersecurity.
- *Cyberzen Desk*: a serious game about the importance of a clean desk in the work environment.

In this chapter, the two games will be presented in depth, aiming for a profound understanding of their nature, their teaching objectives and the experience that the end user receives when they play those serious games. This will aid us to realize not only the cybersecurity principles that are being conveyed to the player, but also allow us to see way it is done, to further evaluate the two games.

3.1 Surf Clean

Surf Clean is an interactive storytelling game which aims to teach the player cybersecurity values in practice. The pedagogical objectives are focused on teaching what social engineering is and in what forms it may appear, by presenting real-life scenarios from the perspective of the victim but also from the perspective of the social engineer. Additionally,

secondary learning objectives include general good practices in cybersecurity, such as password management and secure navigation.

Earlier it was mentioned that *Surf Clean* is an interactive storytelling game, but what does that mean exactly? An interactive storytelling game is one where the storyline is not predefined, but rather it changes based on the choices of the player during the gameplay. In our case, there is a predefined setting for the scenario, to which the player gets introduced initially. The design of the story follows a branching paradigm where each choice may lead to different outcomes but later on in the story, the branches can meet back into common "pinch points" [80]. In this way, the game will pass on the next subject to be discussed in the scenario, even if the player has answered poorly on a previous one. It therefore follows a main storyline which covers specific topics, but each player can have a different experience depending on their choices. An actual depiction of the first 18 questions of a Surf Clean's scenario branching can be seen in Figure 3.1: Inside a black circle there is a question and the blue diamond shape represents a main pinch point. Lastly, the colorful arrows and black arrows represent the possible user answers for each question.

There is a narrator in the role of a coach, guiding the player in the initial and intermediate stages of the scenario, explaining the role that they are going to play, the goal that needs to be achieved by the end of the story and any other information that is needed for following the story. Throughout the storyline, the player is usually given three options to choose from as an answer and rarely only two options. Every choice is significant for the outcome of the story depending on how well it corresponds to the goal of the protagonist in each scenario.

For each story there are three core skills that the player is called to demonstrate in order to succeed their cybersecurity training. Each answer given will affect the rating of one or more of those core skills, either in positive or a negative way. However, this is not revealed to the

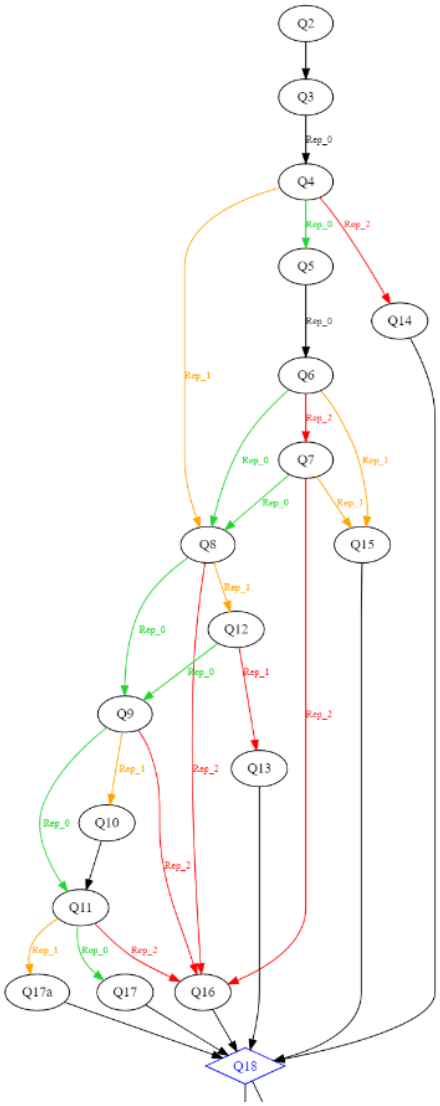

Figure 3.1: Graphical representation of the first part of a Surf Clean's scenario. The diamond shape represents a "pinch point".

player in a direct way, but only through a more generic feedback during the game. The player can see this feedback on their screen after making a choice, with two ways:

- The chosen answer will be colored green if the answer is correct, orange if it is neutral and lastly red if it is wrong (see the colored arrows in Figure 3.1).

- Through the point system, with points being awarded to the player if they have chosen the best answer, or points being subtracted if the answer was unsatisfactory. For the “neutral” answers, no points will be awarded.

For the purposes of this thesis we use the terms “correct”, “neutral” and “wrong” to characterize the quality of an answer. Nonetheless, this does not mean that there is always a correct, a neutral and a wrong answer presented to the player; sometimes, there is more than one correct answer presented and the choice is subjective to the player and/or their organization’s security policy on how to act on specific cases. Other times, a choice is slightly better than another, either because it is better justified or simply because it demonstrates one or more of the core qualities that are being evaluated in each scenario.

While playing each story, the protagonist -the one who the player controls- will build up certain emotions towards their dialog partner, which correlate with the way the player answers. These emotions will eventually affect the responses of the partner, and this will act as an indirect indicator of whether the player is managing to answer correctly or not. For instance, if the player demonstrates poor understanding of cybersecurity fundamentals to their colleague by suggesting using their birthday as a password in order to not forget it, their dialog partner may react to it as it is terrible idea.

When it is the player’s turn to speak, a choice amongst the given options needs to be made in a specified time, otherwise if the timer runs out the answer will be taken as if the player is keeping silent. Player’s silence is typically considered a poor reaction, because they are missing the chance to support their argument and convey their beliefs to their dialogue partner.

From a technical perspective, the game is written mainly in JavaScript (95.4%) while also using some PHP (3.9%), HTML and CSS. It is playable in all modern browsers, such as

Google Chrome, Mozilla Firefox, Opera, Microsoft Edge and Internet Explorer 11. The game is based on the Replica engine, an engine developed by Manzalab Group which is used to create and modify interactive storytelling serious games, depending on the customer's needs and requirements. Finally, the serious game is published by Cyberzen.

Next follows a presentation of each of the three scenarios, for which we will see closer selected parts of the dialogue and their analysis.

3.1.1 Scenario 1: In the shoes of a hacker

3.1.1.1 The story's setting

In the first scenario the player is assuming the role of a hacker. The ultimate goal is to obtain the password of a company's director work email, by convincing the management assistant with some social engineering tricks. In preparation for this social engineering attack, the hacker has collected several information concerning the director, that were readily available on the internet. The game narrator explains to the player that the director is currently travelling in China alongside with his new colleague and cannot be contacted. Additionally, the hacker has found out that his son will be soon leaving for a school trip. Now the player needs to use the collected information to help them with the attack.

3.1.1.2 The three core skills

Instilling trust: A social engineer's primary goal is to achieve building a bridge of trust between them and their victim. Using the gathered information, the social engineer has to progressively create precise and credible arguments to convince their victim to reveal the information that they are interested in. Alternatively, a social engineer may try to play a

riskier game, by creating surprise elements in order to upset and destabilize their victims so that their vigilance drops.

Dramatization: Dramatization is often used by social engineers by describing a very critical situation that needs fast reaction. This is done in the hope of managing to bypass certain security procedures due to the emergency situation they supposedly find themselves into. Often, social engineers will try to manipulate their victims with presenting fictional stories but not necessarily by explaining them explicitly; instead, they may subtly encourage their listener to analyze the situation in order for them to understand the issues that are emerging. Social engineers rely on credible issues and use psychology to lead victims to drop their guard.

Appeal for help: For successfully demonstrating this skill, a social engineer is called to create an empathetic atmosphere between him and his dialogue partner. Successful social engineers have mastered interpersonal communications and will try to appeal for help in sorting out a problem, in the hope of triggering the caring side of their victim and lead them in letting their guard down. Additionally, the desperation that they portray can make them look even more credible when they appear to suddenly have a supposedly "secure" solution which in reality is part of their manipulative plan.

3.1.1.3 The gameplay – Part 1

The hacker first makes a call to the director's office, pretending to be the headmistress of the school that his son is attending. She knows that the phone will be picked up by the assistant of the director and introduces herself accordingly, while subtly introducing the reason for calling: the director's son is leaving for a school trip in 2 hours, but there is a paper missing which needs to be signed by his father beforehand.

When the assistant will ask how she can be of help, the hacker will try to convince her to give the personal email address of the director. This part is very sensitive in terms of how the hacker will handle it, because it can very easily make the assistant suspicious of the intentions of the headmistress and start questioning the fact of whether she is actually talking to the headmistress of the school or to an imposter.

In detail, as it is seen in Figure 3.2, the three given choices at this point are:

a) “Don't worry, everything else is ready I just need Mr. Doucet’s email address.”
b) “I am prepared to send an email to Mr. Doucet’s personal address, but I can't read it from the file.”
c) “We need to act quickly, could you give me Mr. Doucet’s email address, please?”

The first approach by the hacker aims at cutting off the assistant’s intervention to reclaim autonomy in her attempts. While the hacker manages to gain her trust with the reassuring phrase of “don’t worry, everything else is ready”, she misses out on dramatization since her request is not backed up with any details or explanations of the event. This absence of any real justification will be identified as being suspect by the assistant. Questioning about the basis of the request should follow, but there is still a chance to convince the assistant to give away the email address.

As far as the second choice is concerned, it is a smart reaction by the social engineer: the contact’s attention is moved towards the practical circumstances of knowing the address, by a detail of personal circumstances which gives legitimacy to the request. The fact that the address is already given is what creates credibility to the words of the hacker; the assistant is in danger of succumbing because the hacker has created a complicity to resolve the problem in an apparently harmless way: the impossibility of reading the email address due to the illegible handwriting. This answer achieves to increase both the assistant’s trust as well as

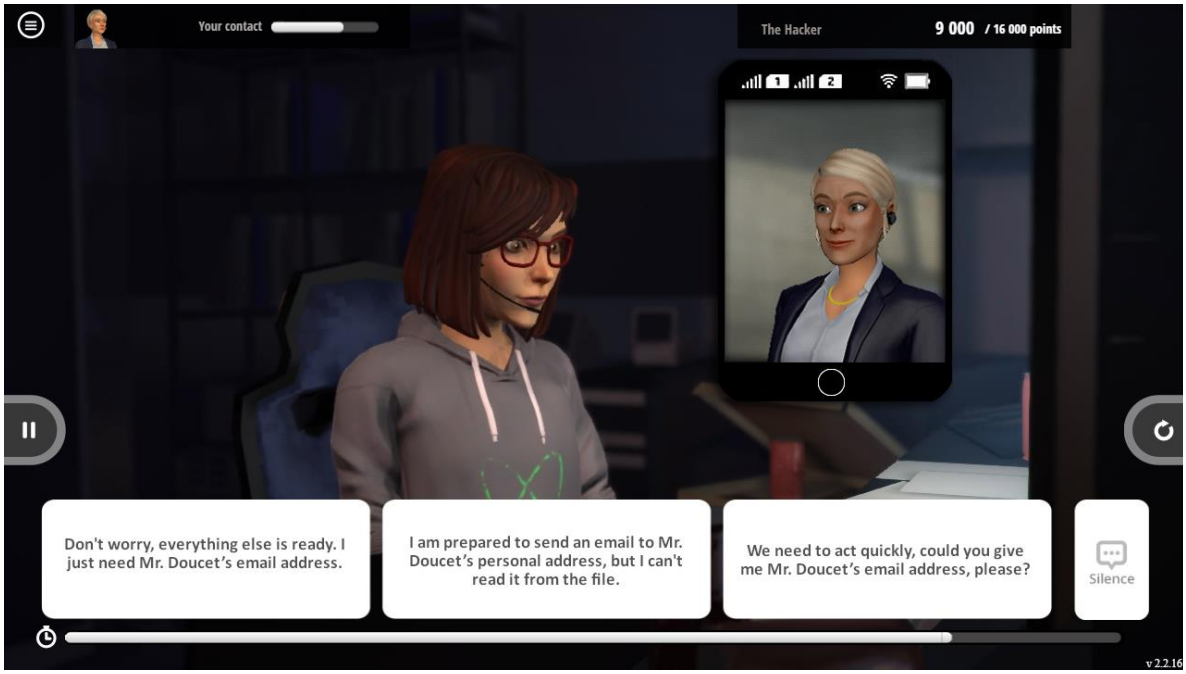

Figure 3.2: In-game screenshot from Surf Clean: the player in the role of a hacker is trying to obtain the director's email address.

managing to appeal for help in a casual way. She agrees that the director's handwriting is sometimes hard to read and volunteers to help the hacker by providing the email address.

The third choice is a very abrupt request, being very poorly linked to any reasons as to why this is a case to act fast. In terms of the three core skills, this answer will affect dramatization negatively, as it is too direct and disconnected from any reasoning. The subject of the request appears to be more important than its usefulness, which provides enough reasons to the assistant to reply with a refusal. Therefore, it is game over since the hacker failed to acquire the director's personal email address.

3.1.1.4 Part 2

If the player manages to convince the director's assistant to provide the email address, the game moves onto the second objective: acquiring the password for the email. For this purpose, the social engineer will now assume the role of a new colleague of the director who is accompanying him in his trip in China. She first introduces herself to the assistant and then updates her on the current situation. Three choices are displayed for the player to choose from:

a) "I am calling you about a serious problem with Mr. Doucet's son's school."
b) "Mr. Doucet has received an urgent email from his son's school."
c) "It seems that Mr. Doucet has received a personal email that he needs to sign quickly for his son's school trip."

The first option represents a good tactic by the social engineer: the way she expresses it is on the one hand precise enough to be credible and on the other sufficiently vague and cautious as to flatter the target's ego. The assistant is therefore in danger as she can imagine herself being in a position of cognitive superiority as she knows that this problem exists. This option boosts the trust towards the hacker but also the dramatization increases due to highlighting the seriousness of the situation.

While the second option closely resembles the first one in terms of dramatization, it lacks the finesse of the first option. The hacker unfolds her plan without taking into account the psychology of the assistant; she is counting on the latter being guiltily passive. If she were aware of the dangers of hacking, the assistant could use this absence of subtlety to identify the attack and question the situation in a very factual way which could embarrass the hacker.

Lastly, on the third option we can see a non-dramatic approach by the hacker, as she trivializes the event. Additionally, it is not accompanied by a request for any particular action;

it is just sending out a hopeful message which undervalues the intelligence of her counterpart. Faced with which the assistant could be naturally disposed to regain her mistrust or treat her with disinterested politeness.

The assistant replies that she is already aware of the situation, as the school headmistress has contacted her earlier. The player then chooses the way to tell the assistant that there is this document that needs to be signed and comes up with an excuse as to why she has to do it instead of the director. The assistant acknowledges the situation, and the hacker explains that the director has given her the password for his personal email address, and a prompt is given to the player to conclude the argument:

a) "…But I can't remember... Look I don't want to have any problems when I've only just arrived... Please. Help me."
b) "He has scribbled it for me on a scrap of paper, but I can't read it. Could you help me please?"
c) "...But I can't remember it and I think that you know it?"

Here, in the first option we can see that the hacker is playing a dangerous game; the appeal for help is clear and straightforward and addresses precise dramatization. It is done with a direct appeal to the emotions, while trying to bring into memory how everyone's first days at a new job can be stressful and chaotic. Be that as it may, the hacker is giving the impression of a colleague who is not worthy of confidence since apparently, she cannot be trusted of keeping something as important as the password of the director safe. Would the assistant want to help someone who is so lacking in reliability? This is gambling on the goodness of her heart or her naivety in believing it.

Concerning the second option, we observe an excellent strategy by the hacker: once again she manages to create a sense of complicity towards the assistant, using a discrete, respectful

criticism of the director’s poor handwriting, which she already knows to be true due to her previous phone call while pretending to be the school headmistress. Moreover, the question "could you help me please?" puts the assistant in a difficult place, where she is facing a straightforward, appealing for help question. The assistant has to be really well prepared to resist this kind of manipulative situation, as the hacker is acting smart by not forcing her hand.

On the other hand, the third choice is a very mediocre attempt by the hacker. The dramatization is as artificial as a hoax call, and the attempt at fostering trust and proximity is strangely crude. The assistant is immediately suspicious with this approach and she answers that unfortunately she cannot help her since this is confidential information that she does not have anyways, and it would be a better idea that the director himself will call her directly concerning this matter.

Afterwards, the assistant makes it clear that unfortunately she does not have the password of the director’s personal email address. The hacker proposes that the director is using the same password for his personal and his professional email address, which is actually the goal of this social engineering attack. The way to do it differs here too, as in one case the protagonist can show confidence in her way of expressing and make the assistant believe that she really has this information, or it can be disastrous if she does not manage to cover well the fact that this was her hidden plan all along resulting in making the assistant skeptical and finally decline her request.

If the player expresses herself in a proper way the game goes on and the assistant now answers that she understands, but nevertheless she is a bit reluctant at giving the password of the director’s professional email address over the phone. The player must now convince her to give the password out to her. A good approach would be to show her desperation in order

to manipulate the emotions of her victim, by showing that she is motivated to do anything that is needed to reassure her.

The assistant is lost in her own thoughts of trying to figure out a solution; this does not allow her to have the necessary objectivity to realize the trap she is falling into, as she starts trusting the person on the other side of the line. The assistant focuses on worrying about the wrong thing: her main fear is that the conversation can be overheard and someone else other than them two may acquire the password. The protagonist grabs this opportunity to come up with a "miracle solution:

"I'm going to send you a secure encryption software that I used to work with when I was at the Ministry of Defense; you will be able to send the password from your computer with no risk whatsoever".

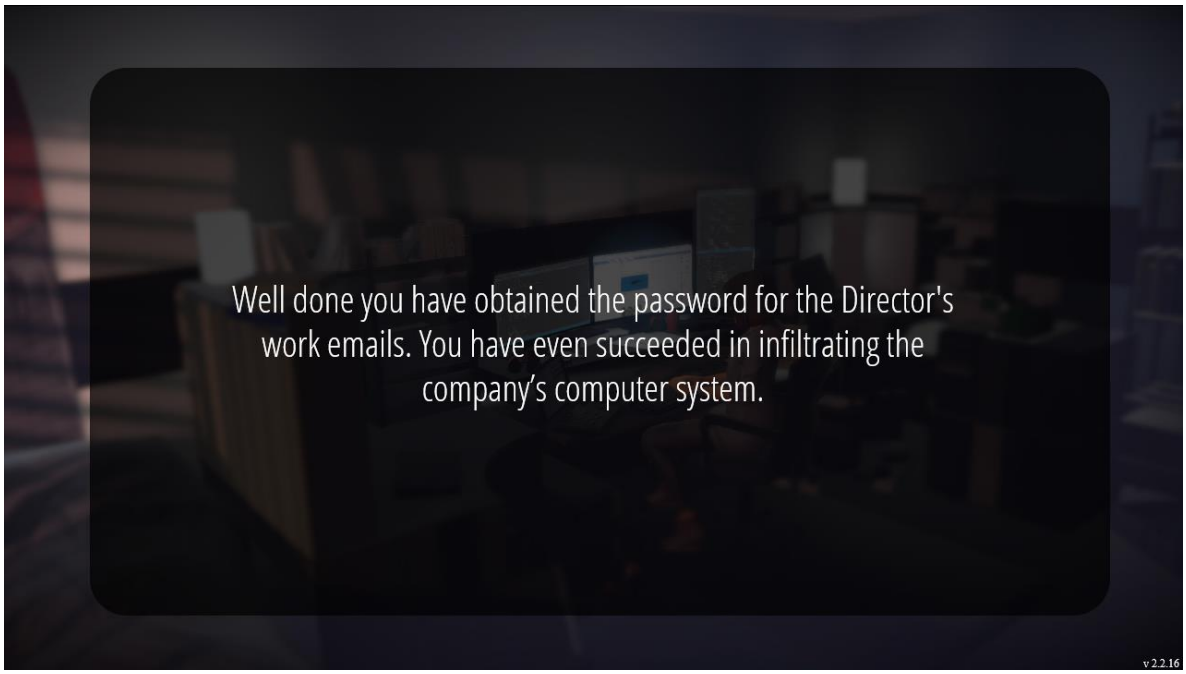

Figure 3.3: In-game screenshot from Surf Clean: the player has managed to successfully finish the first scenario, playing as a hacker.

By using specialized phrases related to computer security such as "secured software", "encryption", "risk-free" and lastly using even the Ministry of Defense to refer to her previous job, the social engineer manages to create a sense of credibility. As a result, the assistant is very pleased with this secure solution that the hacker proposed and accepts to do it in this way.

3.1.1.5 Conclusion

Through this scenario we manage to get an idea of how a hacker thinks when they use social engineering as an initial attack vector. This attack that was carried out in this scenario was not limited on obtaining sensitive information. If our hacker protagonist plays her role well, not only she will manage to acquire the password of the director's professional email, but she will also manage to successfully install a malware software on the network of the enterprise.

Through this "reverse role" scenario the player can observe the manipulation techniques that someone with malicious intentions may use. Additionally, through the goal skills that they are called to demonstrate but also in the feedback provided by the coach in the end of the game, the player can have a better understanding on what goals an attacker has. Lastly, the player themselves can identify the wrong handling of the situation by the assistant. For example, if the assistant had been better prepared about the weapons and methods used by hackers, she would have been able to identify that as a matter of fact, what was presented as secure software offered no actual security.

3.1.2 Scenario 2: A casual discussion about Security Policies

3.1.2.1 The story's setting

The second scenario has a different setting: the player now poses as a bank employee who has been in this company for the past fifteen years. During a coffee break, he meets a newly arrived colleague, Thomas, and starts a casual chat with him. During their conversation Thomas mentions his old university colleague, who also works in a bank and told him how his work computer got hacked recently, due to an infected hyperlink in an email that he received.

Thomas sounds surprised about the fact of how a simple email could have such serious consequences, even though he claims to have read the security guidelines issued by the security department of the bank. He confides to the protagonist that he feels that the security warnings and the dangers that are presented to them are often exaggerated. In this scenario, the main goal for the protagonist is to change the mindset of his colleague by taking a mentoring role and help him understand the importance of following the security policies while showing him the reasons why he should do so.

3.1.2.2 The three core skills

Teaching: Your colleague is new in the company and evidently somewhat naïve in terms of cybersecurity dangers, and more specifically within a financial institution such as a bank. It is essential that the conversation is educational for him and the various risks and issues related to information systems security need to be demonstrated. Moreover, it is important to convince him that the existing security measures are well-founded and not necessarily and exaggeration on the side of the security department. Overall, during the conversation there

should be a calm atmosphere without any dramatization, to ensure that the suggestions for what the best practices are will be clear and thus easily transferred to him.

Knowledge: The second objective is to successfully communicate the knowledge about cybersecurity and the company's policies to the newcomer and present the needed systematic measures which will enable the company to be protected against external threats. It is necessary that the colleague manages to understand fundamental rules of information security, in a clear and precise way. Otherwise, presenting a set of security rules without proper argumentation can look a bit fuzzy or be subject to interpretation which does not allow him to become confident and independent in managing security problems.

Vigilance: Lastly, the protagonist needs to show to his colleague how vigilance is a necessary skill when it comes to fighting threats in information systems' security. It needs to be transparent that it is every employee's duty to be prepared for a cyber attack or phishing attempt but without creating any anxiety to his fellow coworker. The key here is not only to realize when oneself is being attacked, but moreover to understand how to react appropriately in the event of any suspicion of attack.

3.1.2.3 The gameplay

The scenario starts with the two story characters trying to speculate what may have happened to Thomas' friend after opening the infected email attachment. The approach of the player on this speculation can vary in quality; it is important that the answer is not categorical and offers an approach of setting out the multiplicity of risks, in order to address the care that is needed both in relation to the possible consequences of an attack and also in diagnosing the techniques used. It is possible to also suggest that hacking one single workstation is not as insignificant as it may seem, as it can have an effect on the whole company. However, one should not fall into the trap of underlining only a single impact that a cyber attack can have,

such as the financial consequences that may cause to a bank. This type of answer, even if it is not entirely wrong, it is incomplete and somewhat superficial as it is not the only type of consequence that a cyber attack can cause to a bank; other dangers exist as for example threatening customers and their privacy or damaging the overall image of the firm.

The protagonist then has a chance to talk about holding a workstation to ransom. Surprised by this unknown term, Thomas is asking for further information of what this means, and it is time for the player to demonstrate his knowledge by concluding his sentence of what holding to ransom means. The answers given are the following three:

a) "...When hackers pressure a company or individual to obtain money after having stolen or encrypted data."
b) "...When hackers have accessed confidential data and they claim a ransom in exchange for it not being disclosed."
c) "...When you're taken hostage by a hacker."

The first choice is the best possible answer because the player gets the chance to summarize precisely what ransom is ("[It is] when the hackers pressure a company or individual to obtain money") and at the same time explain the way that it is done ("after having stolen or encrypted data"). This answer covers both the goals of being educational as well as demonstrating adequate knowledge of how it is done.

Regarding the second reply, although it is correct, it is not sufficiently detailed. It does not enable the coworker to understand the way this attack method works and limits itself to explaining that the attackers could disclose sensitive information to the general public unless a ransom is paid. Despite the fact that this answer is informational, it does not achieve the goal of successfully displaying knowledge for this topic.

The last choice is obviously a wrong statement; in information security when referring to taking one's computer or device as ransom it is not related to be a hostage of someone. Instead, when there is a ransom attack which is usually done by some ransomware malware, the files on a single computer or a server are encrypted or stolen, and the hackers will try to extort money in exchange of the files. This type of attack can also block the activity of the company for days since they cannot access their data.

The story continues with the dialogue partner saying that in any case if the consequences are not financial, then it should not such a big issue. After all, the important thing is that the security of customers and employees is not affected. It is a great chance for the player to demonstrate their knowledge on the data security topic, by mentioning how serious data theft could be and how it could affect someone's personal life in the case of identity theft or personal data leakage. In particular, this can definitely lead to losing customers' confidence which is very important for an institution which deals daily with such sensitive data, such as a bank.

After Thomas hears the explanations presented by the protagonist, in his reply he seems to be slightly scared of what he perceives to be a huge responsibility to have. He feels that at his level he cannot do much to fight against hackers. The protagonist takes the initiative to show that one of the most important things when fighting cybercrime is to always comply with computer security rules and be vigilant while at the same time keeping a critical mind. It is crucial to show to the colleague that it is everyone's task to make an effort in this because through teamwork, the systems' security is more efficient.

The colleague is quick to answer that computer security mainly tells them not to open strange emails or click on suspicious hyperlinks, but he already follows this instruction. What else is there to do then? The protagonist is called to choose the most appropriate answer to give to him. Seeing that the topic is being careful of what emails to open, it is an opportunity to

mention a very important issue when it comes to judging the quality of an email*: "[...] in any email, the name, address, logo or attachment can be falsified. And paying attention only to that is not sufficient".* Attention is drawn to risks related to fraudulent emails and how they can be phishing attempts targeted to someone in specific. It seems like an appropriate moment to introduce the dialogue partner to the concept of social engineering.

a) "Hackers have a number of ways of harvesting information: in particular from social networks. There, they attempt to break passwords and security questions."
b) "...You can also be hacked via your telephone or any other tool that has already been infected".
c) "...What is absolutely necessary and sufficient to arm yourself against hackers is to comply with elementary security rules."

As a first option we can see a very informative answer about how social networks can be used to mine information that is made public, whether this is concerning a person or an organization. These are data such as photos or texts that people voluntarily upload on the social media, but it does not stop there; even worse, a hacker can attempt to infiltrate someone's personal or professional account by breaking their password or gaining access by guessing the answers to security questions. It is not a rare case that someone may choose to have as a security question something that it is easy to find, such as the name of a pet or the birthplace of their mother which both are often publicly available online.

Regarding the second and the third choices, the answers are not out of place, but they are both too vague and they do not provide any concrete information. The latter is also very confusing for the listener because it gives absolutely no new advice and to make matters worse, it makes him oblivious towards the dangers of social engineering and how easily a hacker can gather data for someone, simply by conducting an online research of this person on the social media. Thus, it has a negative impact on all three core skills that the player

needs to demonstrate in this storyline. The second reply though, manages to at least demonstrate some knowledge skill, but without achieving a teaching objective.

The story continues with Thomas saying that he finds this to be hacking at a high level and that it is very sophisticated. How can he be a target of a criminal para-governmental organization? The protagonist realizes that his colleague is still missing valuable knowledge concerning cybersecurity and its targets. He answers that he is wrong and that nowadays, hackers very often use a technique called social engineering and it is applied directly by telephone or even in meetings. Nonetheless, the target of such an attack can be anyone, from a simple employee to an executive manager.

Afterwards, the protagonist gets the chance to present one of the methods that social engineers use to achieve their goal: aiming to bypass normal security procedures by presenting to their victim any relevant information that they have collected from various sources, in order to reassure them that they are who they claim to be. Thomas is wondering how he can foresee this type of situation and what could be a real-life scenario of this happening, so that he can be prepared to act properly.

Those are the following answers available for the player to choose from:

a) “It could be a hacker pretending to be a customer in a complicated situation or even an up-line manager making an urgent request.”
b) “...It could be someone who is pretending to be someone else and who is aiming to lie to you.”
c) “That’s not important, if you apply the security rules to the letter there's no risk of being hacked and no need to be paranoid either.”

The first option gives an appropriate explanation because it gives actual examples of this sort of attack. It also makes use of the key word “urgent”, since it is often an effective lever to

disturb the attention of a colleague and to make them bypass the rules of security which are to be complied with. Furthermore, describing a person who presents oneself to be in a critical situation should be another alert for a possible social engineering attack.

Once again, the second option is correct in terms of what a possible situation could be, but on the other hand it is not as detailed as the examples presented in the first choice. The main issue with this answer is that due to its vagueness, the colleague who is new to the concept of social engineering may find it challenging to envision a real-life situation based on solely this response.

On the contrary, the third choice is not a fitting reply because it is not really addressing the concern that his colleague expressed on how social engineering is applied in practice. In fact, if this option is chosen, the player will not fulfill his role as a mentor but instead he will promote carelessness and irresponsibility by saying *"that's not important"*. Additionally, he provides his colleague with incorrect information, since it is wrong to imply that following the security rules to the letter will guarantee no risk of being hacked. Some situations like the one described in the first choice cannot be foreseen and written explicitly on a textbook, but they rather require critical thought.

As expected, the newly arrived colleague now raises another important question: how can someone know if a phone call for an urgent request is real and not a social engineering attack? Can one simply rely on recognizing the voice of the person who is on the other end of the line? The player answers that this is not necessarily enough indication to trust someone about whom he claims to be. Principally, a social engineer will put their victim in a position where the latter has the impression that they recognize them but not with certainty.

In addition, the existence of voice masking software makes it impossible to rely only on trusting the identity of a person based on their voice. Therefore, the best clue that one can

have in order to start questioning if someone is telling the truth is to reflect on whether the scenario that the person is presenting to them is essentially forcing them to act outside of normal security rules. Often the person may even give credible details or provide falsified documents that may look legitimate.

Eventually the new colleague starts getting slightly nervous from the new information he receives. He feels that there is actually no reliable way to detect and react on a social engineering attack. Quickly the mentor tries to calm him down by telling him that *"Even though it is hard, there is a good way to counter such an attack…"*, and three choices to complete the phrase are displayed (Figure 3.4):

a) "...Always refuse anything suspicious and send the information to the computer support people."
b) "...Always refuse anything suspicious and send the information to your manager."
c) "...To be vigilant; if there is the least doubt you should check by calling the person back using normal communication channels."

The first two options that are presented in Figure 3.4 are insufficient and not very educational for the listener. The solution of always refusing anything that may seem suspicious which the protagonist suggests is very absolute and does not necessarily tackles the hypothetical situation very efficiently. In any event, for an employee to always decline to cooperate with someone who is asking for their help is a bit risky as it may have the undesired effect of creating a bad impression to the other person who may be genuinely asking for their help.

As far as the second part of the answer is concerned, which is what differentiates the first from the second choice, asking the computer support people is certainly more relative than asking one's manager on how to handle this type of situation. Having said that, it is still not

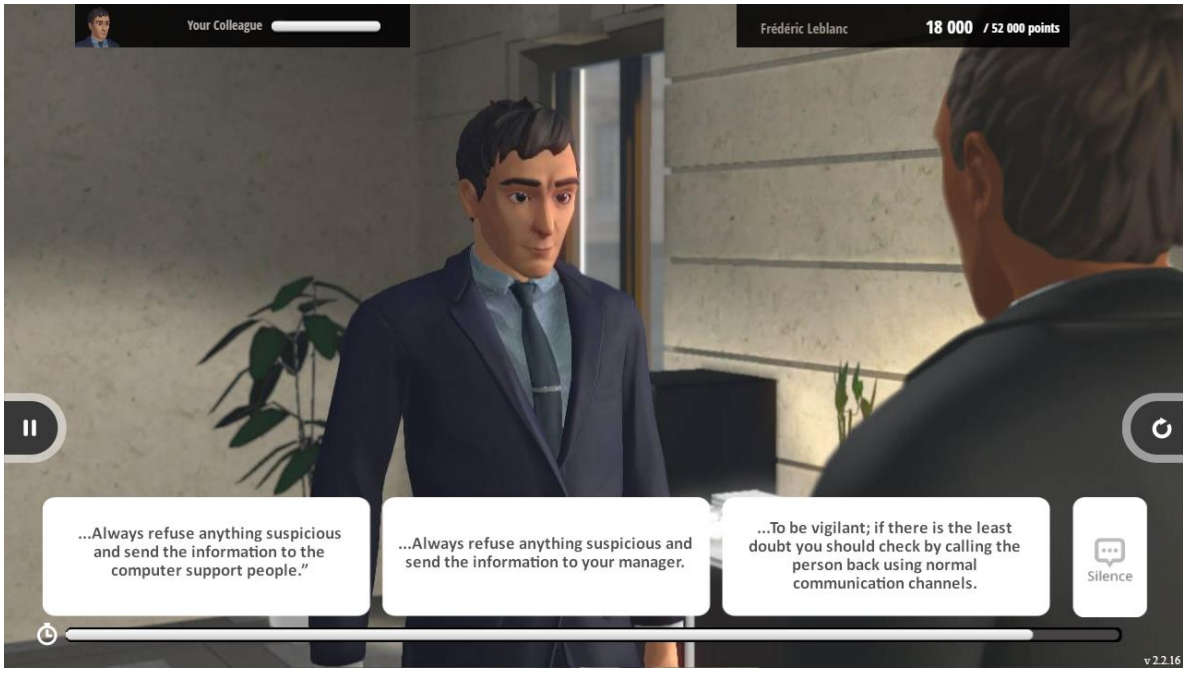

Figure 3.4: In-game screenshot from Surf Clean: the player needs to choose the best way to defeat a social engineering attack

a desired practice to communicate with the security department right away, but first the employee has to assure themselves of the identity of the contact in some other manner. After the necessary checks from the side of the employee who is being contacted have been carried out, the computer support department can be contacted in case there is something suspicious.

On the other hand, looking at the third choice we observe a more mature and knowledgeable answer. The protagonist here suggests a good practice of certifying someone's identity, through a straight-forward technique; calling the person directly on their registered phone number. In general, financial institutions such as banks that very often deal with large amounts of money transfers use two-factor authentication (2FA) for online transactions in a similar way: along with their usual username and password combination, they require another authentication mean which could be an offline verification through another medium such as

a phone call, or an one-time password (OTP) which is sent through SMS, a dedicated smartphone app or a token provided from the bank itself [81].

Supporting the argument of the need to always verify someone's identity without panicking, the protagonist advices his colleague to not give in under the psychological pressure that a contact may put him through, but rather keep a clear mind. There is no need to completely refuse them, only to ensure that they are who they claim to be. This type of answer is both educational and reassuring, while at the same time it encourages him to be careful without falling into counter-productive stress and paranoia.

The protagonist then gets the chance to talk to him about the elementary security rules which can help protecting both himself and the company. He brings up as an example the basic but important rule of never disclosing his password to anyone even if it seems necessary to do so, in order to get something done. Moreover, he advises him to never leave his equipment unattended or lend them to someone as they are strictly personal. In the case of USB memory sticks, connecting them to unknown devices may also pose a security threat so this is also forbidden.

After listening to all the advice that the mentor gave him, the new colleague points out the common issue of how he has trouble with remembering his passwords, because one way or another he might end up forgetting. In that case, one will have to call to the computer department and ask for a password reset, which is a big nuisance. In many cases they will also have to follow a security procedure which includes confirmation text messages and may even result in waiting for a few days before acquiring a new password. He recalls that this is what happened to his sister when she had forgotten her health insurance password and she had to wait for two weeks for a letter with her new password to arrive.

The protagonist is sympathetic to the situation described: indeed, resetting a password may be long and painful but it is just a matter of security. At the same time though, all this can be avoided -or at least minimized- with memory tricks, such as finding his own mnemonic to remember his password. However, his mnemonic techniques should be strictly personal and solely inside his own head; this includes not divulging his password to anyone even if they are trustworthy as well as never noting it down in a post-it note or a file on his computer.

Annoyed by the complicacy involved for merely just a password, Thomas says that he feels that all things considered, there are bigger issues compared to him sharing his password with a colleague, which intrigues the interest of the protagonist to ask him what bigger issue he has in mind. He replies that he has realized the existence of a fault in the security system, since he has administrator rights on his workstation computer which allows him to access some sensitive documents, even though he should not have access to them. The player needs to advise him to communicate this to the helpdesk, as this is a matter of security. It is essential that when such problems arise, they are directly reported to the security experts of the organization to prevent privilege escalation exploits.

The protagonist seizes the moment to ask his colleague a trick question: Who would be, according to his opinion, the most appropriate person to bypass a security procedure on his workstation, in the event of a real emergency? Thomas hesitantly replies that this should be the computer support department. The player needs to correct his colleague, by saying that in reality nobody is authorized to do it, not even the CEO of the company. Baffled, Thomas admits that he did not know that, and that systems security is in fact more complicated than what he had imagined. The player can choose an answer of the following:

a) “No, basically it's logical. You don't put your key under the doormat when you leave home, do you? Well it's the same sort of thing...”
b) “You know, Thomas, these are just the basic rules.”

c) “Yes, you are right, it's complicated. But it's up to you to adapt to the dangers of the modern world!”

In the first option, we observe a metaphor which provides a good reflection of the idea that security rules above all are common sense and are often pragmatic. By doing so, it gives the chance to the colleague to connect a real-life situation of personal physical security to the one of cybersecurity. In addition, it shows that it is a collective effort of all staff members to comply with the security rules to guarantee security throughout the company, in the same fashion that every habitant of an apartment needs to be protective of their own copy of the key.

The second option is incomplete and does not provide the colleague with any kind of critical thinking. Even though the rules set out here are elementary rules, others which are more complicated may exist to defend against complex threats. It is not very educative of him to simply mention that what he just described is really basic without adding something more, such as an example of a more complicated situation. In addition, his dialogue partner could easily get offended by such a non-constructive and slightly arrogant remark.

Similarly, in the third option we witness an insufficient reply. Undoubtedly, it is important to adapt to threats which are continuously evolving. However, agreeing with the colleague on how complicated it is, may give him the wrong perception that there is not much he can do in order to shield himself and the company from the threats that are lurking. Not only this is not educative, but it also shows lack of knowledge on behalf of the protagonist.

Progressing with the story and after having picked the first option presented above, Thomas says that he understands what the protagonist is trying to tell him. Nevertheless, he is afraid that he will not be able to remember all the information he gathered from the conversation that they just had. The player then can choose to motivate him to do a small exercise of

summarizing everything they have just discussed. This approach enables the rules to be assimilated and the measures of care set out previously to be reformulated in his own words.

Thomas lists the essence of their talk: he needs a strong password, not to lend out his equipment and to analyze the messages he receives. Moreover, to not to open emails which have no connection with his work and stay vigilant when there is a suspicious situation. The player should answer that this is exactly it and praise him verbally, as he seems to have understood the measures of care and the procedures to be complied with.

The fellow colleague seems happy with his newly acquired knowledge, but at the same time he seems very worried. He confides to the protagonist that he is afraid that now he will feel a bit paranoid since he is hesitant in trusting his own colleagues now.. The protagonist is called to reassure Thomas, so he explains him that it is not a question of having trust or not, but rather being vigilant for certain situations. For instance, plugging in a USB memory stick which belongs to a colleague or a supplier could potentially infect his computer but that does not necessarily mean that the owner of the stick knows that it is infected. Essentially, he should not always worry about being attacked, but he needs to be aware of the threats in order to be sufficiently responsible, without this meaning that he should be looking for trouble everywhere. Feeling a sense of responsibility implies not only being careful but complying with security rules and adopting best practices.

Thomas seems much more relieved after hearing these explanations. He thanks his colleague for taking the time to clarify all these topics for him, as well as his great guidance and suggestions for best practices.

3.1.2.4 Conclusion

This scenario allows the player to see cybersecurity from another perspective: the one of everyday life. Many employees may find themselves thinking like Thomas when similar situations arise. Thus, through this storytelling experience the player can align themselves to these situations and understand the reasons why following the security policies of their organization is important. After seeing the threats that are presented here, the player will have a better understanding of how to respond to them when it is needed to take some action.

3.1.3 Scenario 3: Security awareness in commercial banking

3.1.3.1 The story's setting

The setting of the third scenario places the player in the role of a client advisor in a commercial bank. The protagonist, Noemie Vialic, is dealing daily with both professional and individual clients. For this storyline, the player has to successfully achieve the twin objective that a client manager has: to comply with the security policies whilst providing qualitative advice and service to the clients.

3.1.3.2 The three core skills

Analysis: In the role of a bank employee that comes in contact with clients daily, it is possible that one may confront cases such those of someone using social engineering techniques to deceive them. Therefore, deep analytical skills are essential for quickly identifying potential risks and managing to confine the situation by asking the appropriate questions and giving the needed answers.

Care: As an employee and more particularly one in a financial institution, it is necessary that all situations are dealt by following the security policies when dealing with client requests. Good knowledge of the right practices is required, but also the motivation to put them in use needs to be shown. Following the security procedures with care, enables oneself to arm the bank against attempted fraud such as financial loss or identity theft. Exhaustive verifications need to be carried out in order to ensure the identity of person who is contacting the individual.

Client relationship: Finally, a skill that every employee needs to possess when they are encountering clients daily is to manage to give them a positive experience during this time. This is easier said than done, because often complying with the security policies requires that the client will be denied some services or be asked to provide some paperwork which may come off as a nuisance. In spite of these difficulties that may arise, an employer needs to remain attentive to the clients' problems and try everything to satisfy their requests as long as they are in accordance to the security procedures.

3.1.3.3 The gameplay: Part 1

One day in the office, Noemie receives an email from one of her professional clients, from an email address that she does not recognize as authorized for the bank. The email reads:

"Good morning Mrs. Vialic,

Could you carry out the following transaction from my business account number 00072YV12, please? 2500€ to my personal account number 00076FF08.

Thanks.

Pierre-Yves Lestrade"

The protagonist thinks that the transfer is internal and quite usual, as Mr. Lestrade is an entrepreneur who travels a lot and makes transfers from his professional account to his personal account from time to time.

The interactive part of the story starts with the player having to answer via email to her client. As a good strategy for such situations, the player needs to ask for some identity confirmation before executing the bank transaction, so therefore she can choose to request from the client to confirm his telephone number before she proceeds with the transfer. The client replies with a short email providing his telephone number and the bank employee completes the transaction. Shortly after, she receives another email from the same client followed by an additional request:

"Could you carry out the following transaction again from my business account number 00072YV12, please? 10 000 € to an account in the name of "Postarak & Co", account number 4466001894 at the Bank of Bothlavia. Thanks."

The player can choose to either allow or deny his most recent request.

a) "I need more information to make this transfer. I am calling you on your reference number."
b) "I'm going to accept this because you are a client that I know well but really you should usually do this online. Next time please download the application."

The first choice reflects a good practice; indeed, when there is something suspicious or unusual concerning a requested transaction it is recommended that the client is being contacted through another medium to confirm their identity. In fact, the client file should show a reference number on which the client should be reliably contacted. This enables the authenticity of the contact to be agreed and thus comply with the principles of client relations management.

On the other hand, the second option falls in the trap of relying on the pseudo-familiarity of the client. In reality, there is nothing that guarantees that the person who is composing those emails is actually the client Pierre-Yves Lestrade. As it has been noted earlier, an attacker can even spoof the email address to show any address by manipulating the "From" mail header. Hence it is a mistake on the part of the employee to allow such an unusual request based on the fact that this is a well-known client, before validating his identity first. Choosing this, the player will complete the transaction and thus fail the first part of this story.

Assuming that the player chose to verify the identity of the caller by calling on the reference number of Mr. Lestrade, the story continues with receiving another email from him as a response:

"I can't, I can't do that on my phone. I don't have a calling extension for foreign countries. I really need to make this transfer. It's a new supplier and there is a risk they'll go to the rival company.

Thank you in advance."

In the email we can observe how the client presents the difficult situation that he finds himself into, and asks for the sympathy of the bank employee. Trying to convince his bank advisor to execute the transaction without the necessary verifications, he mentions that his phone does not accept income phone calls so calling him will be futile, but also points out that the transaction needs to be done as soon as possible. The player must be clear-sighted in order to see through this situation and not let their sympathetic emotions prevail, by denying the transaction but also suggesting an alternative: try using the online banking to complete the transaction safely. Thus, a way out of the problem is offered to the client while following the security protocols at the same time.

The phone rings; it is a foreign number which is not referenced in the bank's records. The protagonist picks it up and Mr. Lestrade is on the other end of the line, calling in reference to her last email in which she declined to execute the money transfer. He seems frustrated and requests to know the reason why the transfer cannot be done.

The advisor replies that she is merely following the usual procedures and she cannot complete the transaction without verifying his identity first. In the context of client relations, it is encouraged to seek for alternatives when it comes to attending to the requests of a client, so an appropriate way to respond to this situation would be by suggesting an alternative way of identity verification: a handwritten request signed, scanned and sent via his authorized email. Note that it is important that the player selects to request that the email is sent from the email that is referenced in his bank contact details, as it is also indicative of his identity.

The client is outraged with the suggestion of the bank employee and explains that he is currently with a new supplier in Bothlavia trying to close the deal. He claims to be situated at the company of his supplier and the security rules there do not allow him to access his online banking or his emails. However, he can nevertheless send her a written request through the corporate email of his supplier instead. In Figure 3.5 the three answers that a player can choose from are presented:

a) "No, that's not possible. Your business seems a bit strange to me."
b) "I'm sorry that's not possible. But you can send it to me from your email address when you get back to the hotel. Or do it online then."
c) "Oh OK, let's do that then: a handwritten letter scanned and signed, sent from your supplier's email address."

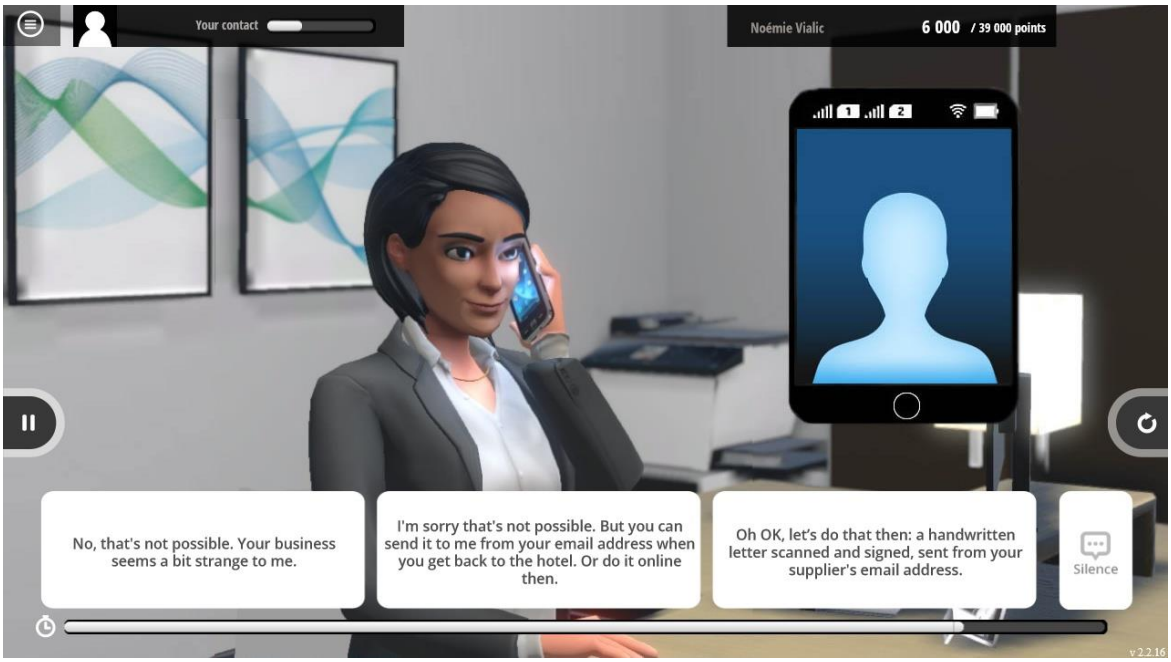

Figure 3.5: In-game screenshot from Surf Clean: the player has to verify the caller's identity according to the security procedures.

Choosing the first option, the player demonstrates some good judgement on refusing to proceed with the transaction. However, when dealing with any client it is important to keep in mind that the relationship with the client and their and satisfaction should be of highest priority hence it is essential that refusing to offer a service should be treated elegantly. If the player chooses this as an answer, the client becomes very annoyed with the behavior of his advisor and an apology accompanied by further explanations are necessary from the side of the employee to continue with the dialogue.

In contrast to the first option, the second reply is both complying with the security constraints for situations like this one, while managing to maintain a good client service by not completely be refusing to execute the requested service. Instead, the advisor offers two alternative solutions that could accomplish what the client requested. This type of answer

achieves to demonstrate all three core skills: analysis of the situation, care but also good client relations.

Examining the third answer, we see that the employee has almost complied with the validation procedures, but without including the security problem related to an email address which is not authorized with the bank. If this answer is chosen, it seems to please the client, but it does not illustrate analytical skills and carefulness from the side of the employee. If this is the choice of the player, the client advisor finally executes the money transfer and the story continues at the second part.

Having chosen one of the two first options, the story will resume with Mr. Lestrade responding that he had already thought of online banking or sending the handwritten consent through his personal email when he returns to his hotel, but it will be too late. The situation is very pressing on his side, because if he does not manage to make the transfer immediately the supplier will sign up with another firm that has already made them a proposal. He explains how time is of huge importance right now and that he is need of her help. Moreover, he says that he understands how this situation is a bit extraordinary, but he makes an appeal on their long-term acquaintance of ten years. Usually, he adds, he handles those transfers himself and just this one time that he asked for her help, she is refusing to support him, so what is she even useful for? Those procedures are completely stupid, he adds.

It is evidently a very tough situation that the bank employee finds herself in; her client is very frustrated and stressed to see this transfer happening in order to seal the deal with his supplier. Mr. Lestrade is playing all his cards to manage to convince her: firstly, he underlines the time pressure he is under. Secondly, he implies that he has been a great client for many years and never caused her any similar issues therefore she owes him this one small favor. Lastly, he tries to attack her personally by making her feel useless for not being able to assist him in his time of need, all because of those security procedures which seem useless to him.

The player needs to stay alert and not let their personal feelings prevail when hearing this monologue from the frustrated client. In response to this, the player should choose to answer that the only solution that does not require the client to have an internet connection is to call him from the phone number which is registered with the bank. The client does not get any happier with this response and he continues attacking his advisor:

"So does that mean I have to tell you in Bolthavian, or what? I do not have my telephone; I don't have any extension for foreign use. But surely you recognize my voice, don't you? So, what's the difference with what's usual? I'm just calling you from another number!"

This is an opportunity for the protagonist to explain to her client the reason why she cannot permit this request of money transfer to be executed, by telling him that recognizing his voice is not enough evidence for her to confirm his identity, as anybody could be pretending to be him and even imitate his voice. Through this answer, the player illustrates their knowledge of this identity theft technique which justifies her unwillingness to simply carry out the task that he requested.

Nevertheless, Mr. Lestrade does not seem to share her beliefs for the security measures she is following. He replies that this is unbelievable and never in his life has he seen such a thing. He is clearly disappointed and warns her that they will definitely talk about this again when he returns. The advisor has no other choice but to wish her client to have a good day and finish the phone call.

3.1.3.4 Part 2

A few minutes later, the protagonist receives another call from a personal client of hers, Mrs. Marechal, who is a pensioner. The bank advisor greets her and asks her how she is feeling, as she knows she recently had an operation on the hip and the old lady replies that she is

recovering fine, at least considering her age. Afterwards, she presents her the reason why she is calling: her granddaughter is currently setting up her first home with her husband. She continues with providing a few more personal details in the story, so she corrects herself, saying that maybe it is more appropriate to call him her friend and not her husband, since they are not married but rather have a civil partnership that claims that they are living together. Nevertheless, seeing that they have just rented a two-room apartment in town she would like to offer them some financial aid as a gift, and thus she would like to make a transfer of 5000 € to her granddaughter's husband.

The bank employee asks her if she has ever used the online banking service, since it could help her to do exactly what she just described, but the old lady replies that she does not know how to use it. The player sees the following choices to continue the story:

a) "In that case the simplest thing to do is to come to this branch."
b) "Because as I'm sure you'll understand I can't make a transfer for such a sum over the phone like that."
c) "But actually why do you want to make the transfer to your granddaughter's husband rather than to her directly? That's strange…"

The first reply is the best possible answer because a visit to the bank in person will ensure the identity of the application and therefore allow the transfer to be made without any issue.

The second reply is not ideal because even though the employee explains that she cannot make the money transfer over the phone due to its great amount, she does not offer an alternative to her client, which is what the client wants to hear at this moment. Thus, such an answer may endanger the relationship that she has with her.

The third option is a poor reply on behalf of the employer: she is questioning the legitimacy of the transaction which is being requested and indirectly expressing doubt on the honestly

of her client. Granted that her job is a client advisor, she is not fulfilling her duties but rather endangering her professional relationship with her client. Mrs. Marechal is clearly bothered with this answer, asking her how is this any of her business and telling her that in fact she can do anything she wants with her money. An apology will be necessary before continuing with further explaining her what she can do to make the transfer happen.

Assuming that the player has chosen to suggest to her client to come to the local bank branch, Mrs. Marechal answers that this will be a bit complicated for her due to her recent operation on the hip. Even though the operation went well, she is still unable to move, let alone leaving her house to go to the city. The player is presented with the choice of suggesting to her to give her some proof of her identity, and for this she will need to see a handwritten letter, scanned, signed and sent via email, accompanied by a scan of her identity card. The client seems happy to hear that there is an alternative way to treat her request. She says she will do this right away, she thanks her for her time and hangs up the phone .

Soon after the protagonist receives an email with the documents that she requested, which confirm the identity of Mrs. Marechal. The player is confronted with a dilemma: make a call back to her referenced phone or execute the transfer directly? Choosing the latter is not conforming with the security procedures, because a hacker could have easily obtained or falsified such documents and waited for an opportunity like this to use them. In case the player chooses to make the money transaction, the third scenario passes onto the third part of the story. However, as soon as the third part is over, there is a follow-up to Mrs. Marechal's story which will be presented later, in chronological order.

On the other hand, if it is chosen to verify the legitimacy of the client's identity by placing a phone call to her referenced number, the player will find themselves facing a surprise: Mrs. Marechal picks up the phone, but she does not seem to recall requesting for a money transfer earlier this morning. It is a very delicate situation to handle and it must be done with the

needed care because the protagonist should not stress her client with the news. It is therefore not advised to rush into conclusions and not tell her client that she has been hacked yet because it is very abrupt, and it will cause her a lot of stress. Besides, it is not even established yet that she has been a victim of hacking or identity theft.

It is more appropriate that the player chooses to cancel the transfer right away and investigate further on this matter, by asking her if she had been asked to provide any personal information recently. Mrs. Marechal recalls receiving an email last week from Noemie herself, asking her for a handwritten letter and a scan of her identity card which she provided immediately, within the delay of one day.

The protagonist informs her that it was not her who requested those documents, and this unfortunately means that she was probably the victim of hacking. Afterwards, the player can choose to ask her to forward the email to her, so she can transfer it to the department which deals with situations as such. Choosing this, the player demonstrates a good analysis of the situation in suspecting a fraudulent email. Moreover, it informs her client that the investigation is not over, and that it will be taken seriously by sending it to the department which is specialized in dealing with such cases. Mrs. Marechal agrees to do that, and they end the phone call.

3.1.3.5 Part 3

Later in the day, another client who uses the bank for both personal and professional matters, calls to inform Noemie that his mobile phone got stolen last night. Unfortunately, all his information was on it, including the password to his online banking. As an advisor, lots of care is needed to ensure that the reaction is not excessive in a way that it may scare or infantilize the client. Instead, the player should choose to keep a calm tone while sympathizing with the client and show that she is available to help him. The client appreciates

the interest shown and replies that the reason he is calling is in fact because he wishes to change his password. There are three ways that the protagonist can choose from to do that:

a) “I'll have to immediately send it to you by mail.”
b) “Well now, you need to go to your online banking site and then you can replace your password.”
c) “In that case I'll send you a new password by SMS immediately.”

The first option complies with the communication procedures that involve requesting a new password to be created. Indeed, these types of requests need to be communicated to the department that is responsible for managing the online banking accounts and is authorized to send out the new password via mail home address of the client.

The second reply is not an appropriate answer on behalf of the advisor; if a client can't identify themselves on the online banking site, they won't be able to change their password. Choosing this reply will have an impact on the client relationship, because it does not demonstrate a sufficient level of listening and care.

Concerning the third option, it is a poor choice for a three-fold reason. Firstly, the phone is not in the possession of the client anymore, so the SMS would never reach him, thus the client will perceive this as inadequate care to his problem which will hurt the client relationship. Secondly, no password can be sent directly by the advisor over to the client’s mobile phone, so this shows lack of knowledge in handling such situations. Most importantly though, when examining this action from a security perspective, it is undoubtedly a reckless move to send the new password on a stolen phone.

After resolving into deciding to send the new password via mail, the client is not satisfied with this proposal because it will take a lot of time with traditional mail and he will be blocked since he uses daily the online service. The protagonist in turn suggests that the other option

would be for him to go to a local branch of the bank and get the password directly. However, this still does not fit the schedule that the doctor has, since he works during the opening hours of the bank and it is not possible to cancel the appointments with his patients in order to do this. The client's counterproposal is to receive the new password by email, which is instant.

The player needs to patiently explain to her client that this is not possible because the possibility of his email having been hacked is very high and it would be better to avoid sending such sensitive information to it. Nevertheless, this is not the reply that the client was expecting; for him this is not convenient, and he is seemingly annoyed that he will have to resolve at being blocked out of the service until he receives his new password through mail. He demands to speak to her manager to help him figure out another solution. The protagonist answers that the manager is currently in a meeting, but she will have him call the client back when he is available. Concerning the password, she adds, it will be automatically replaced and soon he will receive the new one by regular mail. The client, annoyed, greets her and hangs up the phone.

3.1.3.6 Part 4 – Follow-up of part 2

The last part is a small telephone conversation that is playable only if the player has chosen to proceed with the transaction that Mrs. Marechal has requested in the second part of this story. A few days later, Mrs. Marechal calls the advisor regarding a strange transfer of 5000 euros that she noticed in her bank statement. She seems confused concerning this record, because she does not know what it is for or where the money went. The protagonist explains that she approved the transfer after having received a request from her three days ago to transfer this amount of money, followed by an identity verification via email. As suspected, the client replies that it was not her who called her, nor did she send her any emails as she was out of town visiting her son.

Throughout this phone conversation it is needed to keep calm and not cause any panic to the client. Hence, even if by analyzing the situation it seems that Mrs. Marechal has been a victim of identity theft, the player needs to choose the dialog options that include questions which can be used to successfully identifying if this is actually the case and how it happened. Once again, provoking unnecessary anxiety to the client before verifying the suspicions of hacking may possibly complicate or even totally obstruct the situation analysis.

The dialogue that follows is quite similar with the one described in the second part of the story, in the path where the player chooses to place a phone call to her client before executing the requested money transfer. Similarly, by asking the right questions such as whether Mrs. Marechal was prompted to give out any personal information or whether she could forward the phishing email which she received, the player manages to reassure her client that the case will be treated with the utmost urgency and by the appropriate department which investigates and treats those financial frauds. Mrs. Marechal agrees to do that, and they end the phone call.

3.1.3.7 Conclusion

Through this analysis of the scenario we can see how sometimes it may be complicated to maintain a balance between good client relationships while adhering to the security principles. Many clients that the bank advisor talked to were not happy that they were denied the service they requested due to security procedures. One client even requested to address to her manager, which sometimes may scare an employee who feels they may get in trouble for not satisfying the needs and requests of their client, and finally succumb into granting them their wish just to avoid this case.

However, having deep knowledge of the actual security procedures should give the confidence to the employee to not deviate from their original position of declining the

request, knowing that their manager will approve of this act. Furthermore, a good client relationship can be maintained by suggesting alternative solutions that are still aligned with the security policies of the organization, or trying to resolve the clients' issues with step-by-step analysis while asking the appropriate questions to guide towards a solution.

3.2 Cyberzen Desk

Cyberzen Desk is a 3D Virtual Reality (VR) experience thatcreates an immerse environment for the player, which closely resembles a possible real-life situation. The setting of this game is in a typical work office, where the player is portraying an adversary who has physically broken into the offices of a bank and tries to find anything that could be valuable, such as a USB stick, confidential documents etc. The purpose of this game is to convey the importance of a clean desk and alert the employees on what information someone malicious could steal in their offices if they do not handle their personal and professional items with the appropriate care. All this is delivered through a fast-paced scenario where the player is called to identify signs of non-compliance to the security policies in the office.

This game has been designed by cybersecurity experts from Cyberzen team in collaboration with game designers, scenarists and developers from Manzalab Group, using the Unity game engine and C# as programming language. The teams were following the business needs of a big French bank for employee cybersecurity awareness and were in constant communication. The virtual reality game was a complementary part of the cybersecurity awareness campaign, which was initially delivered to the employees first through lectures and awareness posters in the workplace and finally enhanced with this game. As far as game localization is concerned, the game was first developed and released in French language, and then translated into four more languages: English, Dutch, Italian and Estonian.

The game begins with very little introduction: the player can see that they are in an office in front of a desk, and can hear the narrator speaking to them. The narrator explains that the

break-in was successful and now the player has to look for anything useful that the employee may have left behind. For each object that is found, there is a brief explanation which indicates why having it easily accessible causes a security breach. This commenting that can be heard during playing time, is coming from the partner in crime who is also encouraging or giving hints to the player if they seem to be stuck while time passes by. The time for searching in the targeted office is limited to three minutes, so the player needs to be rigorous, analyze fast the situation and start "hunting" for items that could be possibly violating the security policies. After the gameplay is over, there is a summary overview which is fully customized to give the appropriate feedback based on the performance that the player had.

The camera view of the game is from a first-person perspective, which means that the player can see and experience everything from the perspective of the protagonist. The camera movement is controlled by the VR headset which, combined with the first-person perspective, is what gives the realistic sensation to the overall game feeling. Concerning the player input towards the game, it is accomplished by fixating the center of the screen onto an object that can be interacted with, and after a short delay the interaction happens. The interactable objects are discerned from the non-interactable objects, with the visual change of the icon that is present in the center of the screen. The icon will transform from a dot to a circular loading bar which fills up while the user is fixating on the object, as can be observed in Figure 3.6.

There are two types of actions that can be applied on interactable objects: the player can take the object to examine it closer or perform an action such as opening a desk drawer to investigate what there is inside. For each object that the user interacts with, there is a feedback from the story narrator, depending on its usefulness in their goal to hack the bank or sell valuable information to other powerful competition in the financial market. The player does not know the list of the items that they are supposed to find while searching the office, so critical thinking is needed to determine where to look in the allotted time.

Figure 3.6: In-game screenshot from Cyberzen Desk: the player is inspecting the docking station key and the laptop that goes with it.

Some of the exploitable items that can be obtained are listed below:

- Smartphone: A smartphone nowadays is comparable to a personal computer, therefore if acquired and hacked by someone it may give access to personal and professional email, contacts or other confidential documents which are saved in there.

- A docking station for a laptop and its keys: a docking station is a piece of hardware that is often used in offices to easily plug-in a laptop device and instantly connect the screens, external keyboard or other hardware to it, in one move without managing all their cables every time. This device gives access to the laptop and its hard drives and can be physically exploited, in a similar way of skimming an ATM device; adding a device which reads all the data passing through and transfers them back to the attacker. It is considered to have multiple reasons for an attacker to target it, since they often exist in environments where it is usual to change desks many times per day, and therefore gives access to multiple laptop devices. Moreover, their constant power supply ensures a continuous communication to the malicious server but most importantly, it can gain access to encrypted data after they have been decrypted when they reach the laptop and the end user [82].
- Confidential document in the trash bin: The trash bin is considered a mine of information for hackers: it is very important not to simply throw away papers which contain sensitive information, but rather shred them instead. A confidential document may include information that can be afterwards sold to the competitors of the bank and result in a deal failing, for example. In this case the burglars can find a merger & acquisition plan with confidential third-party information for which the bank has most probably signed a non-disclosure agreement. Leaking of such information could lead to many hazards for the bank and their clients (Figure 3.7).
- List of names and numbers written on the whiteboard: With the first glimpse it is not obvious what could be of use from the information written on the whiteboard but taking a fast picture of it for future analysis can potentially be lucrative for hackers.
- Professional badge: A professional badge is essentially a physical key that opens all the doors in the building and potentially give access to other buildings too. Moreover, it is also a digital key too, as the holder can gain access onto the bank's network by using it to start a new session on a computer. It is therefore strictly personal as it also

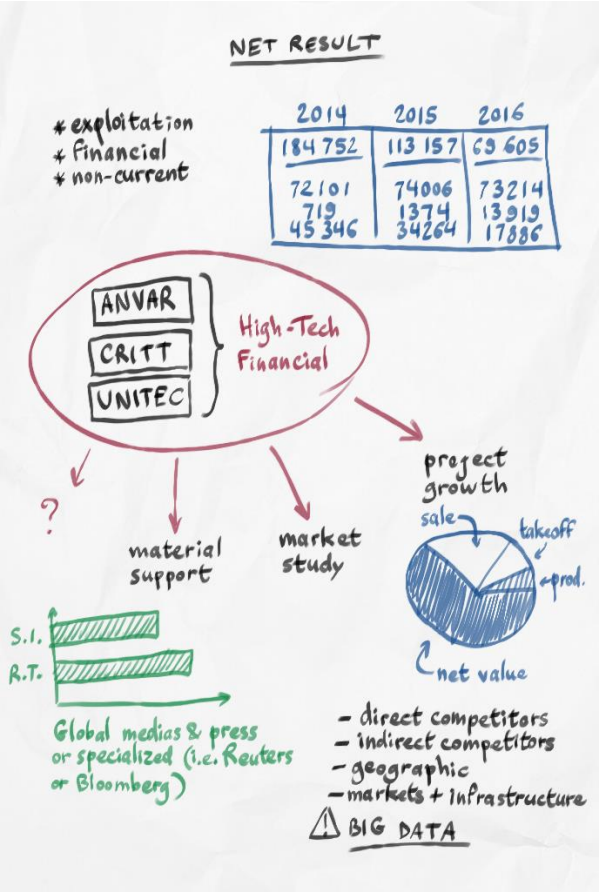

Figure 3.7: In-game item from Cyberzen Desk: A confidential document found in the trash bin.

leaves behind a digital print every time it is used, so the actual badge owner can be tracked and be blamed for any damages or losses that may happen.

- Password on a post-it note: It may sound improbable but it is still a recurring issue with employees and their passwords. The number of different passwords that they are called to use, only increases the chances for someone making the mistake of writing down their password and leave it in play sight. Similarly to the professional badge, a password that will grant access to a computer or server will leave a digital print behind and the employee will be accused for any illegal activities. Instead of writing down the password or a post-it or on a computer document, it is advised that the employees will use a password manager instead.

- Encrypted USB stick on the desk: Even if encrypted, a skilled hacker could manage to gain access to a USB stick used within a bank and retrieve valuable information from it. Relying on the fact that it is encrypted should not be an excuse for not storing it in a safe location.
- Notebook with sensitive information: A notepad that is used professionally should not be left in plain sight due to the fact that it may contain sensitive information. In this case, the burglar managed to obtain a notepad full of client names and details, as well as secret bank strategies.
- Conference call card: A conference call card can allow a person to host or participate in a conference call. Much like a badge, it is strictly personal and it should be kept safe at all times. Otherwise, if it gets stolen by someone with malicious intentions, it can be used to spy on confidential meetings and extract sensitive information that could reveal strategies and internal decisions of the company.
- Token Secure ID: A token is a physical device which is used to securely login in a platform, as part of a two-factor authentication (2FA). If the adversary succeeds in getting hold of both the token which generates a one-time password as well as the normal password, then they can gain access into the internal network of the bank.

Moreover, the player can interact with some furniture in the environment, such as the drawers of the desk or the cupboard in the office, to search for the aforementioned items. In addition to these, there are also interactable objects that are not useful such as a post-it with a shopping list, a note for a personal appointment or a keychain but without any keys attached on it (Figure 3.8)

During the game, the player does not see a timer of his exact time remaining to complete his mission. Instead, there are two time-triggered verbal reminders from the narrator, who has been acting as the player's partner in crime; one reminder is after the first thirty seconds have passed and it is given in case the player has not yet managed to find any useful items, that

Figure 3.8: In-game items from Cyberzen Desk: Items that the player can find that act as distractive factors. (a) a shopping list (b) a personal medical appointment

hints the player to look around and suggests searching any cabinets or drawers for things they can use.

Moreover, when the timer reaches two minutes, the partner will again remind the player to hurry up because time is running out and the security guard will be arriving soon. As soon as the three minutes are over, the narrator announces to the player that there is no more time and they must leave because he can see the security guard approaching. However, in case that the player finds the ten items that are considered exploitable, the game is over before the end of the three minutes.

In the end of the game the narrator goes over the things that the player did not discover during the three-minute office inspection. For each undiscovered item the player can see where it was hidden in the office, and an explanation of how this could be a potentially valuable source of information is given to the player. Moreover, depending on the performance that the player has had, a personalized feedback is given along with an overview of the generic problem that was faced during this game: a work desk which does not comply with the security guidelines, which leads into the exposure of many sensitive information. Afterwards, the good practices

are presented to the player when it comes integrating the habit of a sanitized work environment: always lock your computer session, keep your professional badges and devices securely stored or with you, ensure the destruction of certain sensitive documents before discarding them, and more.

4 Results

The two games that were presented earlier, *Surf Clean* and *Cyberzen Desk*, are commercial off-the-shelf (COTS) serious games so they were therefore designed and developed based on the needs of certain types of organizations, as mentioned before. Moreover, this posed another restriction: it was not easy to collect data on their overall effectiveness or the end user satisfaction, as the games' primary purpose was not to conduct an academic research while using them, but rather to serve the needs of the organization for cybersecurity employee training.

However, one of organizations who used *Cyberzen Desk* as part of their cybersecurity training, a private health insurance company in France, created and conducted a questionnaire to the people who took part in this training programme, and had the courtesy of sharing it with Manzalab Group. The survey provides feedback on the players' general perception and satisfaction of the training session. There were 66 participants that took part in the survey, after having taken part in the cybersecurity training session, in which *Cyberzen Desk* was used among others.

The presentation of the following results has been adapted by the author of this thesis to match its purposes and conceal the identity of the company. Additionally, all the content of the survey has been translated from French to English by the author herself. However, the

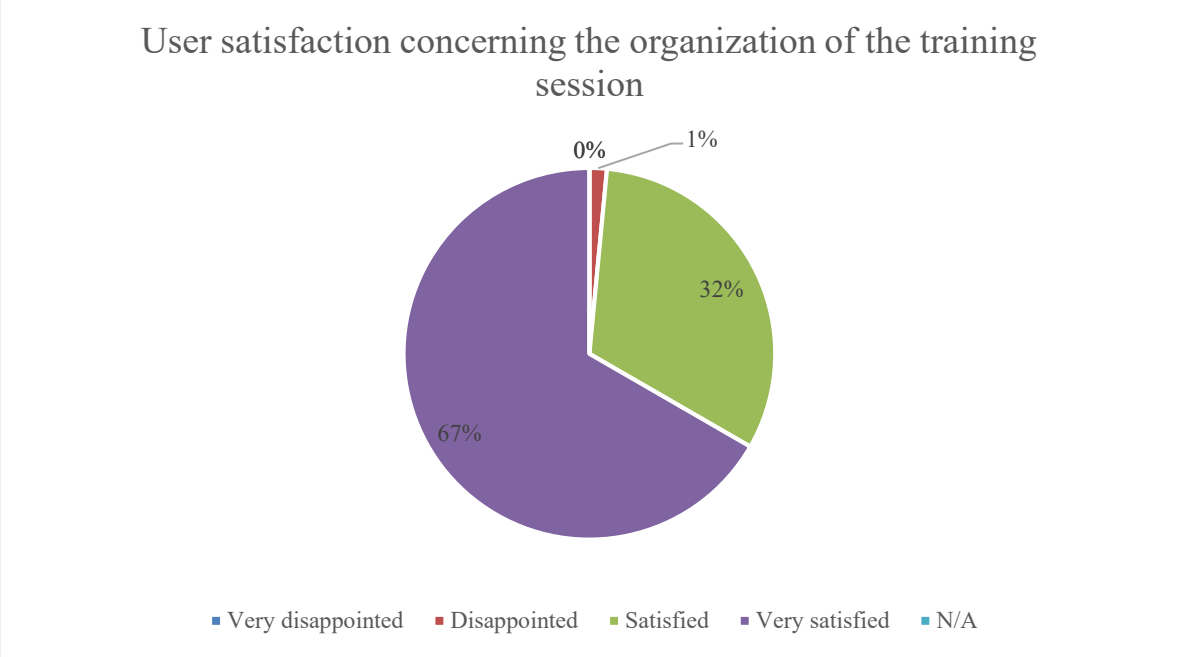

Figure 4.1: User feedback on their satisfaction levels for the organization of the cybersecurity training session (Source: internal survey after the cybersecurity training programme)

results presented here are genuine and reflect exactly the survey results that were granted by Manzalab group and the insurance company for the purposes of presenting them in this thesis.

To begin with, looking at Figure 4.1, we can initially observe that users found the organization of the cybersecurity training session that was hosted internally by the insurance company to be very good. Almost all the participants answered that they were satisfied or very satisfied with the organization of the training session. However, in the section where the users could give their feedback in the form of a comment, someone asked to better organize the scheduling of the sessions, in order to avoid waiting time. Another participant proposed that the training sessions can take place multiple days, so that people who are working remotely when the cybersecurity awareness day takes place, can still participate.

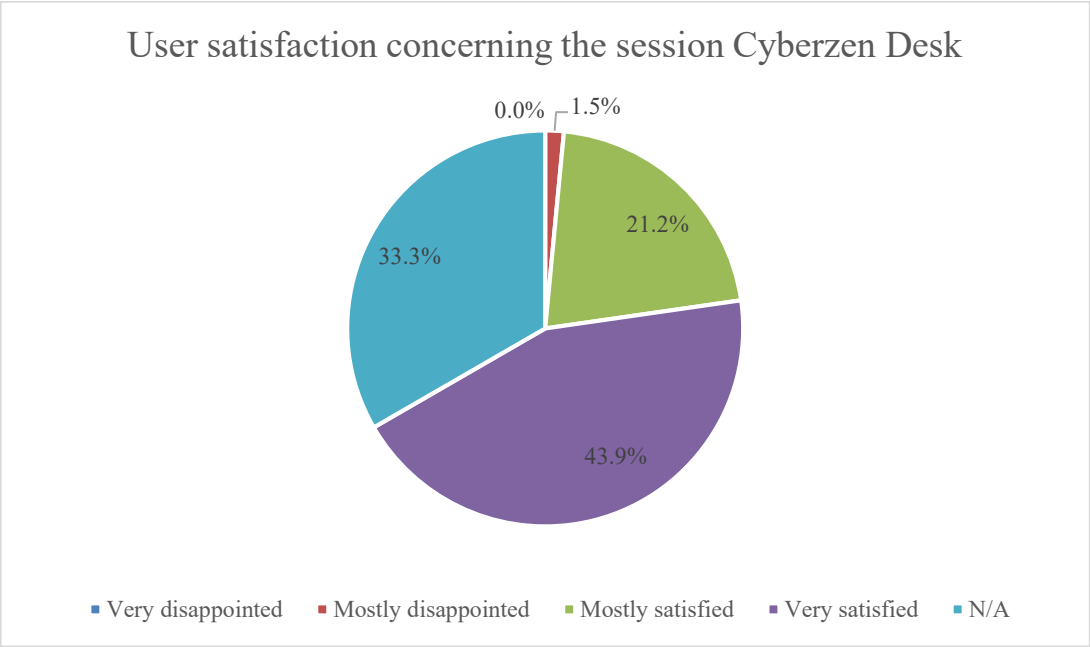

Figure 4.2: User feedback on Cyberzen Desk session. (Source: internal survey after the cybersecurity training programme)

As seen through Figure 4.2, 65.2% of the participants answered that they were satisfied or very satisfied from their experience of playing the VR game *Cyberzen Desk*, which accounts for more than 97% of the participants who chose to answer this question.

However, 33.3% of the participants did not provide any relative feedback. Comparing this result with the one in Figure 4.1**,** we can assume that the people who chose not to answer this question possibly did not participate in the *Cyberzen Desk* session. Only 1.5% of the participants said that they did not enjoy that session.

On another topic, it is interesting to see what were the actions that motivated the employees to take part in the cybersecurity training programme (Figure 4.3**)**. The employees were asked to select the means which incited them to participate in the training programme, with the ability to select multiple answers. The answers are ranked from 0 to 7, with 7 being the motives of highest importance for the employees. People said that the most important factor

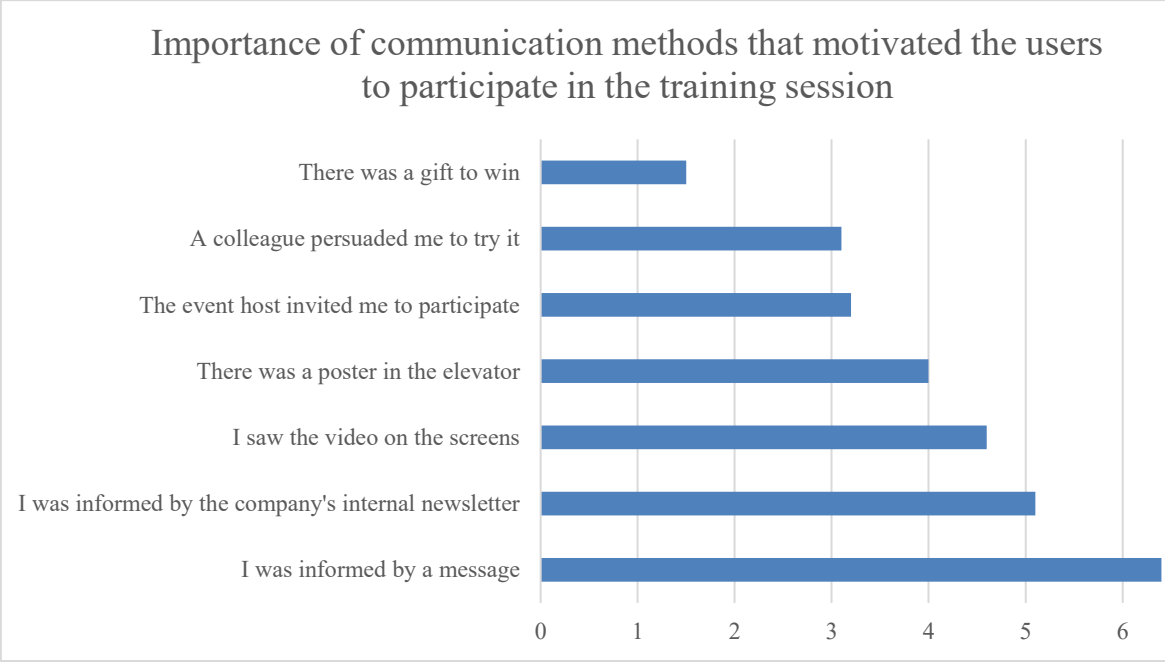

Figure 4.3: Motivation sources for the employees to participate in the session (Source: internal survey after the cybersecurity training programme)

in their decision to participate was being notified through some message or reading about it through the internal newsletter magazine of the company.

Nevertheless, even though it is important to inform the employees through the more traditional ways, it seems that projecting the event's information through a video on the screens or on a poster is also relatively important.

On the other hand, incentivizing employees to participate due to the possibility of winning some reward, was the least important reason for the participants. This comes as a surprise because in the literature we had seen that adherence to security policies could be more successful if there was a tangible reward involved [54]. Although participating voluntarily in

the cybersecurity training is not precisely promising adherence, it does align with the intention of self-improvement on security concepts.

Moreover, in terms of content quality and content relativity the participants were overall happy with almost two out of three employees saying that the session was qualitative and also relevant (Figure 4.4). As far as aesthetics is concerned, 70% of them found the session aesthetically pleasing and attractive.

It is worth looking deeper into the information provided by Figure 4.4 and more specifically to the feedback concerning what the people think of the overall usefulness of the session. Even though a very small portion of people thought that it was not useful, almost 40% of the people were undecided about its usefulness, and barely a bit more than half of the participants

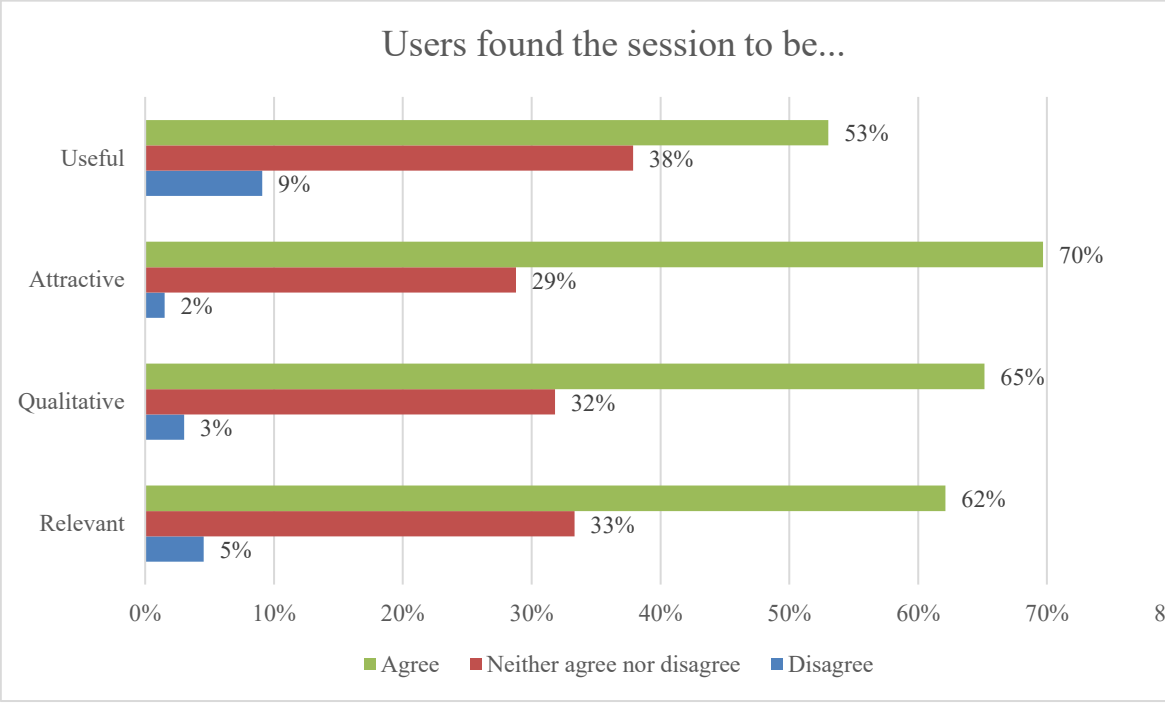

Figure 4.4: User perception on different evaluation indices of the training session (Source: internal survey after the cybersecurity training programme)

thought it was useful. So, a question here arises: what could have been done better? Why did some participants feel that the content was not useful?

Looking at the section where the employees could freely give their input about the cybersecurity training session, we see two pieces of feedback that could give us a hint about that issue:

"Give examples that are more related to our profession, we are not in NASA.", Anonymous.

"It would be interesting to have more realistic elements to better understand the security risks in the work environment.", Anonymous.

From the above, we can observe that two people thought that the content of the session was not ideal for their profession. The difference of the scenario compared to their real daily job seem to have caused them some trouble following or relating to the training session. Even though this should have been reflected also on the relevance index of the session, it could have been as well the reason why some users thought that the training was not so useful after all.

Be that as it may, positive feedback was also present in the survey results concerning the usability. Another participant found the session to be an "excellent way to simulate a situation" and that "it can be used in multiple projects". Other comments relevant to the *Cyberzen Desk* VR session were as following:

"Very playful workshop with an equally reasonable duration. The important points are discussed. An experience to repeat", Anonymous

"[An] original idea to raise employees' awareness. [I am] happy to have experienced virtual reality.", Anonymous

“Continue training us with the new methods!”, Anonymous

In addition to the information presented above, the survey also provided some more feedback concerning the user impression. All the participants were called to grade their overall experience on a scale from 1 to 5 and the final grade was an average of 4.2. What is also interesting is that when the participants were asked if they would recommend this training to a colleague, 97% said mostly yes. Equally, 94% of the people seemed eager to participate in a next session. All these extremely high numbers show that the training session despite its small issues, was a success, at least in terms of user experience and satisfaction.

5 Discussion

Taking into consideration the feedback received from the satisfaction survey concerning the cybersecurity training session where *Cyberzen Desk* was used, but also the literature that preceded this research paper, we can draw a few conclusions about how people perceived it, what was done successfully and what needs more improvement.

To begin with, people seemed to appreciate the short duration of the game. This generally correlates with the literature [56], where we had already seen that trainings with lengthy and traditional forms of communication do not appeal to people. Moreover, we can observe that the 3D VR environment was very welcome by the audience: the attractiveness index rating as well as the mentions in the free comment section seem to confirm this. The choice of a new technology to convey the importance of a clean desk to the employees seemed to have worked as intended: the crowd was immersed and did not perceive the training as an annoying task to complete.

Another point concerning the short duration of the game is that it puts the player under pressure and urges them to think fast and not lose focus. The flow [72] is evident as the player focuses on the single, clear goal they have: locate and gather anything that the person who works in this office might have forgotten and may pose a security threat. The element of flow together with the independence of the player's actions, makes this a tier-three type of game, based on the three-tier model that Gestwicki and Stumbaugh proposed in their paper [60].

From a usability and UX point of view, the game consists of a very simple user interface and the player can interact with the objects around them simply by looking at them for a short duration of time. The narrator gives constant feedback to the player, which was deemed the most popular and therefore important factor when it comes to successfully designing a serious game with the help of a framework [66]. The player will hear the narrator giving them hints when they are stuck, time notices to inform them that the time is running out and praises for managing to discover the things that hold valuable information for the bank or can be exploited by the attackers for money profit. Even in the case that the player picks up items that are not carrying any significance in terms of information and exploitability, the narrator will keep the mood lightweight by making some humoristic comments.

On the contrary, some participants expressed doubts about the content of the game: they did not find it appropriate to their actual jobs. The game is indeed, set up in a totally different environment: the offices of a bank. Even though the sensitivity of a bank's files can be compared to a patient's files and the importance of clean desk is equally great in both types of job, it is nevertheless true that some of the physical items that are found in a typical office in a bank, might be missing from a private insurance company; similarly, some of the policies or processes that are followed by a bank may not be familiar to some organization with a different main activity.

Additionally, the comment that mentioned *"We are not in NASA"* can possibly insinuate that this person found the content of the training harder than he expected and felt that it was somehow too advanced for them. This can be an issue, because as we had seen in the literature concerning security education [19, 8] and serious games [68], it is essential that in order for the training to manage to keep the user immersed throughout its duration and finally have an optimal effect, it needs to be neither too easy nor too hard for them. Nevertheless, there was only one comment that implied the existence of this issue, but it should still be considered in the future improvements of the training session.

On the other hand, and examining this closer from a game design perspective, the game difficulty is not flat even if it seems so through its simplistic goal: *"find the items that may pose a security threat"*. Having a single goal and the freedom of looking around and interacting with things in the environment at one's will, does not necessarily mean that there is no escalation in the game difficulty. The items that are spread in the environment have different difficulty ranking. While some items can be considered very evident to some people (e.g. the post-it with the user's password on it), others are less obvious and require critical thought or more actions on the side of the player (e.g. the encrypted USB stick which is hidden within the cupboard behind the desk), so it follows the variance in difficulty as proposed in the framework by Kiili [68].

In the case that a player did not manage to find certain items within the time frame, there is a detailed feedback in the end of the game, showing one-by-one the items that the player missed by highlighting them in the environment, and explaining why this item is considered a threat to cybersecurity and to the reputation of the firm. The guide will also explain to the player what the appropriate action or behavior is when handling such items. For instance, a sensitive document needs to be shredded before it is disposed. This type of feedback still has an educational output and it summarizes the points that the player missed.

As far as *Surf Clean* is concerned, since we do not have any user feedback related data available to present, we can instead review the strengths and weaknesses of that serious game based on the points mentioned in the literature. *Surf Clean* is aiming to train employees on detecting social engineering attempts through different roleplaying scenarios. The game teaches through narration and the player is able to choose through a finite amount of answers for each situation; that classifies it as a tier-two serious game in the model proposed by Gestwicki and Stumbaugh [60].

Surf Clean prepares the player for cases where similar conversations may take place in real-life, so that the player will be equipped to identify them and hopefully avoid them. Mitigating such an attack is a great accomplishment, because as we have established in the literature the human element does indeed pose a great security threat [5].

Yet, according to the three-tier model [60] a cybersecurity professional, or in our case someone who is confronted with a cybersecurity-related issue, will never have some pre-defined options presented to them when they have to make a decision. As a result, the person who receives this type of training may be prepared for situations that closely resemble the ones presented in the game but may be caught by surprise when other, unfamiliar situations arise. This is evidently a shortcoming of this type of games and consequently for *Surf Clean.*

Regarding the feedback within the game, it is also immediate but transferred to the player through a different way compared to *Cyberzen Desk.* When the player chooses an option, they will have visual feedback on how appropriate their answer was: The bubble which contains the answer they selected will be colored either green, orange or red, depending if it was a correct, neutral or wrong answer respectively. Additionally, in the case that the user answered correctly some score points will be awarded, but in the case of a wrong answer some score points will be removed instead from the total score of the player in the running scenario.

In the first type of feedback we see that the feedback is immediate and very visible to the player, like suggested in the literature [66]. It is clear to the player at that moment that the answer is appropriate or not for this type of situation which can help them remember it in a possible future scenario. This may be useful for situations where the player chose the correct answer, but a restriction is the case where the user chooses the neutral or even worse, the wrong answer. The problem that we identify here is that the user may not know which is the best way to handle the situation they find themselves in. Even though there is a final summary

of the scenario in the end of the game which goes through all the players choices in detail and explains the reasons why an answer is appropriate or not, it is possible that the player might not retain all the mass of information given at that moment.

Making a choice on how to handle the situation presented to the player through the scenario in the virtual world, is essentially no different than the actions that the player could perform in the real world. We can therefore draw a parallel between the aforementioned score point system and the rewarding or sanctioning a behavior in regard to security policy obedience, as we saw in the literature [8]. Nevertheless, even though this game follows this logic of rewarding and sanctioning, we still cannot draw a conclusion on whether this type of feedback will motivate the player to adhere to the security policies due to the lack of user feedback after playing the game.

One of the strengths of *Surf Clean* is the fact that its design is flexible and easily scalable. The game was built using the Replica game engine which was developed by Manzalab Group, and can therefore be used indefinitely to keep adding new scenarios and teach different cybersecurity concepts according to the needs of the customer. This allows an organization to schedule several training sessions and present new content which will incite the employees' interest with the option to mix it with recurring content to monitor the employees' evolution in these cybersecurity concepts. Repeating a training is considered to be very important to ensure that the employees follow the right security principles long-term [8] [57].

Another possibility is that the organization can leave it up to their employees to schedule their own training time, as there is no need for an instructor or special equipment, which is the case for VR serious games. Thus, each employee can choose the best fit in their own schedule and complete the session; the average duration of a scenario is around 5-10 minutes. This should be very appealing to the employees, if we recall that for *Cyberzen Desk*

satisfaction survey there have been comments that mentioned its short duration as a very positive element, while another person expressed their complaint about the waiting time for participating in the training session.

6 Conclusions and Future Work

The games presented in this paper were adapted to cover the needs of cybersecurity training in financial institutes and so the scenery and the events are happening in a bank's office. However, the security topics that are conveyed are broader and therefore playable by employees in other fields as well aiming to have a positive impact in understanding the importance of cybersecurity and following the policies as instructed by the company they work at.

In our case, the scenario of the game *Cyberzen Desk* is taking place in a bank, but it was also used successfully as part of the training program in a private insurance company. Nevertheless, when deemed appropriate and to create a more relatable feeling to the player [8], the games could be easily enhanced by introducing environments and scenarios that are more fitting to their real-life situations. Consequently, further research questions arise from this point: does the end user relatability to the game protagonist and environment affect their overall success in the educational program? What other types of organizations could be grouped together when designing a serious game on cybersecurity?

Cyberzen Desk conformed with most of the best practices in terms of both teaching cybersecurity principles and designing a serious game. Concerning the guidelines that were

reviewed in the literature section, the game can be characterized by its short duration and at the same time its immersive, state-of-the-art 3D VR environment. From an educational point of view the game is focused on one clear goal: keeping a “clean” desk at work; a desk that no valuable information can be gathered by a third party at any given point.

On the other hand, *Surf Clean* is much simpler in terms of gameplay and the technologies used, which can be considered both a strength and a weakness for different reasons. While a simpler gameplay can seem boring for more experienced players, it might seem more accessible to people with not much experience in gaming. Consequently, this can help them focus on the narrative and the learning objectives instead of getting frustrated with learning more complex game mechanics. Also, the fact that *Surf Clean* is playable through a browser gives the player the freedom to access it and play it at their own convenience. In the end, the primary purpose of the storytelling scenarios is to train the employees for stressful situations so that if they happen in reality when the danger is real, the person will be prepared and will be able to react appropriately.

For both games there is an immediate feedback when the player performs an action, but also a detailed feedback in the end of the game, which explains the points missed by the player paired with an explanation of what the good practice is. However, there is some concern around this point: is the end summary enough for the player to understand the good practices? What if it suddenly feels as an extensive load of information to the player, which may potentially minimize the learning outcome? In regard to *Surf Clean,* should there maybe exist more feedback as to the reason why a choice is wrong during gameplay time? This knowledge gap that is identified here, could be covered with some additional future research accompanied with a player survey, to understand better the effectiveness of learning and of course enhance the overall user experience.

More questions arise when we revisit the topic of rewarding or sanction an employee behavior. In a sense, rewarding is very common in games as well as serious games, but sanctioning (i.e. reducing score points) is not encountered very often. This small detail could be easily parameterized for future tryouts of the game and have different user groups which will play the game with or without sanctioning, to later express their feelings through a questionnaire. Since this is easier and less dangerous to apply in a virtual world through a training session for cybersecurity, we can afterwards use it to answer questions such as if sanctioning wrong behaviors is a smart tactic to apply in an organization.

This master's thesis primarily focuses on the presentation of two serious game designs which have been commercially used inside large companies as part of their cybersecurity awareness programs. Even though they are designed while aiming at overcoming many of the shortcomings of traditional employee education, there were not enough post-training data to analyze and review how well these games manage to succeed in those aspects. Moreover, due to the fact that this paper has been written based on archival data and no new organizations used the abovementioned games at the time of writing, it was impossible to conduct a survey designed solely for the purposes of this research. This is an obvious limitation for drawing conclusions about topics such as what was the actual impact that this training session had, or how often should it be repeated in order to have constant results, and further research should be made in order to address the efficiency of using serious games as part of cybersecurity education.

To sum up, through this paper we explored the weaknesses of human element and saw how they can be exploited by adversaries. Employee training against these threats can significantly help mitigate the risks, but it does not have to be mundane for the participants: serious games can be used instead of traditional and outdated training methods. Two serious games were presented in depth; the first one focuses on teaching what social engineering is and what is the right way to respond in such situations. The second game aims to convince

the player to care about keeping a clean desk in their office, while making them see the danger through the eyes of a malicious attacker who will steal anything of informational value.

After having reviewed the weaknesses of traditional teaching methods, it is more evident that by using serious games many of those problems are resolved. Initially, due to the faster pace of the games, the sessions can be much shorter but also more fun for the learner due to the gamification factors. Additionally, through the games the employee can experience more realistic situations than when reading through a textbook. Nonetheless, creating a game still requires a pedagogical structure and a solid game design framework in order for it to be successful in overcoming those problems.

7 Bibliography

[1] B. Barrett, "An Astonishing 773 Million Records Exposed in Monster Breach," 16 January 2019. [Online]. Available: https://www.wired.com/story/collection-one-breach-email-accounts-passwords/. [Accessed 2 February 2019].

[2] S. Schroeder, "You can now browse through 427 million stolen MySpace passwords," 1 July 2016. [Online]. Available: https://mashable.com/2016/07/01/myspace-password-database/. [Accessed 3 February 2019].

[3] L. Franceschi-Bicchierai, "Another Day, Another Hack: 117 Million LinkedIn Emails And Passwords," 18 May 2016. [Online]. Available: https://motherboard.vice.com/en_us/article/78kk4z/another-day-another-hack-117-million-linkedin-emails-and-password. [Accessed 3 February 2019].

[4] L. H. Newman, "4-Year-Old Dropbox Hack Exposed 68 Million People's Data," 31 August 2016. [Online]. Available: https://www.wired.com/2016/08/hack-brief-four-

year-old-dropbox-hack-exposed-68-million-peoples-data/. [Accessed 3 February 2019].

[5] S. Lineberry, "The Human Element: The Weakest Link in Information Security," *Journal of Accountancy,* vol. 204, no. 5, pp. 44-49, 2007.

[6] L. Marinos and M. Lourenço, "ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends," European Union Agency For Network and Information Security (ENISA), 2019.

[7] Cisco 2018 Annual Cybersecurity Report, "The defender landscape," Cisco, 2018.

[8] A. Nagarajan, J. M. Allbeck, A. Sood and T. L. Janssen, "Exploring Game Design for Cybersecurity Training," in *IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems*, Bangkok, Thailand, 2012.

[9] O. Chiang, "Wombat Security Makes Online Games That Teach Cybersecurity Awareness, Nabs $750,000 US Airforce Contract," Forbes, 8 October 2010. [Online]. Available: https://www.forbes.com/sites/oliverchiang/2010/10/08/wombat-security-makes-videogames-that-teach-cybersecurity-awareness-nabs-750000-us-airforce-contract/. [Accessed 9 October 2019].

[10] HealthIT.gov, "Privacy & Security Training Games," HealthIT.gov, [Online]. Available: https://www.healthit.gov/topic/privacy-security-and-hipaa/privacy-security-training-games. [Accessed 9 10 2019].

[11] Naval Postgraduate School (NPS), "CyberCIEGE: Can you keep the network alive?," [Online]. Available: https://my.nps.edu/web/c3o/cyberciege. [Accessed 2 October 2019].

[12] NOVA Labs, "Cybersecurity Lab," NOVA Labs, [Online]. Available: https://www.pbs.org/wgbh/nova/labs/about-cyber-lab/. [Accessed 2019 October 9].

[13] Cyber Realm, "GenCyber Card Game: Cyber Realm," [Online]. Available: https://gencybercards.com/. [Accessed 2 October 2019].

[14] NSPD-54/HSPD-23, "Cybersecurity Policy," The White House, Washington, 2008.

[15] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Computers & Security,* vol. 38, pp. 97-102, 2013.

[16] J. Andress, The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, Syngress, 2011.

[17] D. Clark, T. Berson and H. S. Lin, At the nexus of cybersecurity and public policy: some basic concepts and issues., Washington, DC, USA: The National Acacdemic Press, 2014.

[18] OWASP, 2017. [Online]. Available: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf.

[19] D. Ashenden, "Information Security management: A human challenge?," *Information Security Technical Report,* vol. 13, no. 4, pp. 195-201, 2008.

[20] Special Publication (NIST SP) - 800-12 Rev. 1, "An Introduction to Information Security," National Institute of Standards and Technology, Gaithersburg, US, 2017.

[21] International Standard (ISO/IEC 27000:2018), *Information technology — Security techniques — Information security management systems — Overview and vocabulary,* Geneva, Switzerland: International Organization for Standardization (ISO), 2018.

[22] M. Kjaerland, "A taxonomy and comparison of computer security incidents from the commercial and government sectors," *Computers and Security,* vol. 25, no. 7, pp. 522-538, October 2006.

[23] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta and Q. Wu, "AVOIDIT: A Cyber Attack Taxonomy," in *9th Annual Symposium on Information Assurance*, Albany, NY, USA, 2014.

[24] J. D'Arcy, A. Hovav and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research,* vol. 20, no. 1, pp. 79-98, March 2009.

[25] M. Erbschloe, Trojans, Worms and Spyware: A Computer Security Professional's Guide to Malicious Code, E. Inc., Ed., Oxford: Butterworth–Heinemann publications, 2005.

[26] W. Gao and J. Kim, "Robbing the cradle is like taking candy from a baby," in *Proceedings of the Annual Conference of the Security Policy Institute*, Amsterdam, Netherlands, 2007.

[27] "An overview of social engineering malware: Trends, tactics, and implications," *Technology in Society,* vol. 32, no. 3, pp. 183-196, August 2010.

[28] Special Publication (NIST SP) - 800-53 Rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations," National Institute of Standards and Technology, Gaithersburg, US, 2015.

[29] A. Prakash, M. Ovelgonne, S. V. Subrahmanian and T. Dumitras, The Global Cyber-Vulnerability Report, S. I. Publishing, Ed., 2015.

[30] N. Weaver, V. Paxson, S. Staniford and R. Cunningham, "A taxonomy of computer worms," in *WORM '03 Proceedings of the 2003 ACM workshop on Rapid malcode*, Washington, DC, USA, 2003.

[31] L. Bridges, "The changing face of malware," *Network Security,* vol. 2008, no. 1, pp. 17-20, January 2008.

[32] A. Zimba, L. Simukonda and M. Chishimba, "Demystifying Ransomware Attacks: Reverse Engineering and Dynamic," *Zambia ICT Journal,* vol. 1, no. 1, pp. 35-40, December 2017.

[33] R. Shirey, "Internet Security Glossary, Version 2," IETF RFC 4949, August 2007.

[34] T. Jagatic, N. Johnson, M. Jakobsson and F. Menczer, "Social Phishing," *Communications of the ACM,* vol. 50, no. 10, pp. 94-100, 2007.

[35] A. Aleroud and L. Zhou, "Phishing environments, techniques, and countermeasures: A survey," *Computers & Security,* vol. 68, pp. 160-196, 2017.

[36] C. Kang Leng, Y. Kelvin Sheng Chek and T. Choon Lin, "A survey of phishing attacks: Their types, vectors and technical approaches," *Expert Systems with Applications,* vol. 106, pp. 1-20, September 2018.

[37] R. Dhamija, J. D. Tygar and M. Hearst, "Why Phising Works," in *Proc. SIGCHI Conf. Human Factors in Computing Systems (CHI '06)*, Montréal, Québec, Canada, 2006.

[38] M. Alsharnouby, F. Alaca and S. Chiasson, "Why phishing still works: User strategies for combating phishing attacks," *International Journal of Human- Computer Studies,* vol. 82, pp. 69-82, 10 2015.

[39] M. Tyler and C. Richard, "Examining the Impact of Website Take-down on Phishing," in *Proc. Anti-phishing Working Groups 2nd Ann. eCrime researchers summit (eCrime 07)*, Pittsburgh, Pennsylvania, USA, 2017.

[40] CERT Coordination Center, "Multiple web browsers vulnerable to spoofing via Internationalized Domain Name support".

[41] V. A. Díaz, "MX Injection - Capturing and Exploiting Hidden Mail Servers," Internet Security Auditors, White Paper, 2006.

[42] M. Kumar, "WARNING – New Phishing Attack That Even Most Vigilant Users Could Fall For," The Hacker News, 15 February 2019. [Online]. Available: https://thehackernews.com/2019/02/advance-phishing-login-page.html. [Accessed 17 March 2019].

[43] C. Tracey, "Spear-phishing: how to spot and mitigate the menace," *Computer Fraud & Security,* vol. 2013, no. 1, pp. 11-16, January 2013.

[44] K. D. Mitnick and W. L. Simon, The Art Of Deception: Controlling the Human Element of Security, Indianapolis: Wiley Publications, 2002.

[45] Australian Government, "Hacking Motives," Australia, 2005.

[46] G. Ollmann, "Hacking as a service," *Computer Fraud & Security,* vol. 2008, no. 12, pp. 12-15, December 2008.

[47] R. Madarie, "Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers," *International Journal of Cyber Criminology,* vol. 11, no. 1, pp. 78-97, January – June 2017.

[48] M. Colesky and J. Van Niekerk, "Hacktivism: controlling the effects," in *Annual Conference on WWW Applications*, Durban, South Africa, 2012.

[49] H. Dixon, "British 15-year-old gained access to intelligence operations in Afghanistan and Iran by pretending to be head of CIA, court hears," 19 January 2018. [Online].

Available: https://www.telegraph.co.uk/news/2018/01/19/british-15-year-old-gained-access-intelligence-operations-afghanistan/. [Accessed 19 February 2019].

[50] Special Publication (NIST SP) - 800-37 Rev. 1, "Guide for Applying the Risk Management Framework to Federal Information Systems," Gaithersburg, US, 2010.

[51] M. Bishop, "What Is Computer Security?," *IEEE Security and Privacy,* vol. 1, no. 1, pp. 67-69, January 2003.

[52] S. Pahnila, M. Siponen and A. Mahmood, "Employees' Behavior towards IS Secur ity Policy Compliance," in *40th Annual Hawaii Intl. Conf. on System Sciences (HICSS'07)*, Hawaii, US, 2007.

[53] D. W. Straub, "Effective IS Security: An Empirical Study," *Information Systems Research,* vol. 1, no. 3, pp. 255-276, September 1990.

[54] L. Kirsch and S. Boss, "The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines," in *Proceedings of the 28th International Conference on Information Systems (ICIS 2007)*, Montreal, Canada, 2007.

[55] G. Dhillon, "Managing and controlling computer misuse," *Information Management & Computer Security,* vol. 9, no. 4, pp. 171-175, 1999.

[56] M. Eminağaoğlu, E. Uçar and Ş. Erenc, "The positive outcomes of information security awareness training in companies - A case study," *Information Security Technical Report,* vol. 14, no. 4, pp. 223-229, November 2009.

[57] T. Caldwell, "Making Security Awareness Training Work," *Computer Fraud & Security,* vol. 2016, no. 6, pp. 8-14, 2016.

[58] J. Smed and H. Hakonen, "Towards a Definition of a Computer Game," Turku, 2003.

[59] D. W. Shaffer, K. Squire and R. Halverson, "Video Games and the Future of Learning," *Phi Delta Kappan,* vol. 87, pp. 104-111, October 2005.

[60] P. Gestwicki and K. Stumbaugh, "Observations and Opportunities in Cybersecurity Education Game Design," in *2015 Computer Games: AI, Animation, Mobile, Multimedia, Educational and Serious Games (CGAMES)*, Louisville, KY, USA, 2015.

[61] C. C. Abt, Serious Games, New York: Viking Press, 1970.

[62] D. Michael and S. Chen, Serious Games: Games That Educate, Train, and Inform, Boston. USA: Thomson Course Technology PTR, 2005.

[63] K. Corti, *Gamesbased Learning; a serious business application,* PIXELearning Limited., 2006.

[64] D. Djaouti, J. Alvarez and J. P. Jessel, "Classifying Serious Games: the G/P/S model," *Handbook of Research on Improving Learning and Motivation Through Educational Games: Multidisciplinary Approaches,* pp. 118-136, 2011.

[65] F. Laamarti, M. Eid and A. E. Saddik, "An Overview of Serious Games," *International Journal of Computer Games Technology,* vol. 2014, p. 15, 2014.

[66] C. Tsita and M. Satratzemi, "Conceptual Factors for the Design of Serious Games," in *International Conference on Games and Learning Alliance (GALA 2018)*, Palermo, Italy, 2019.

[67] S. de Freitas and S. Jarvis, "A Framework for Developing Serious Games to meet Learner Needs," in *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2006*, Orlando, Florida, 2006.

[68] K. Kiili, "Content creation challenges and flow experience in educational games: The IT-Emperor case," *Internet and Higher Education,* vol. 8, no. 3, pp. 183-198, 2005.

[69] S. de Freitas and T. Neumann, "The use of 'exploratory learning' for supporting immersive learning in virtual environments," *Computers & Education,* vol. 52, no. 2, pp. 343-352, 2009.

[70] K. Kiili, S. de Freitas, S. Arnab and T. Lainema, "The Design Principles for Flow Experience in Educational Games," *Procedia Computer Science,* vol. 15, pp. 78-91, 2012.

[71] F. Bellotti, R. Berta, A. de Gloria, M. Ott, S. Arnab, S. de Freitas and K. Kiili, "Designing Serious Games for education: from Pedagogical principles to Game Mechanisms," in *5th European Conference on Game-Based Learning*, Athens, Greece, 2011.

[72] M. Csikszentmihalyi, Flow: The Psychology of Optimal Experience, H. &. Row, Ed., New York, 1990.

[73] "Privacy & Security Training Games," HealthIT.gov, [Online]. Available: https://www.healthit.gov/topic/privacy-security-and-hipaa/privacy-security-training-games. [Accessed 9 10 2019].

[74] Science Applications International Corporation (SAIC), "CyberNEXS Global Services," [Online]. Available: http://the-advice.com/images/CNEXS.pdf. [Accessed 2 October 2019].

[75] C. E. Irvine, M. F. Thompson and K. Allen, "CyberCIEGE: Gaming for Information Assurance," *IEEE Security & Privacy,* vol. 3, no. 3, pp. 61-64, 2005.

[76] C. E. Irvine and M. F. Thompson, "CyberCIEGE: A Video Game for Constructive Cyber Security Education," *Call Signs, a publication of the United States Naval Aerospace Experimental Psychology Society,* vol. 6, no. 2, pp. 4-8, 2015.

[77] G. Jin, M. Tu, T. H. Kim, J. Heffron and J. White, "Game based Cybersecurity Training for High School Students," in *49th ACM Technical Symposium on Computer Science Education*, Baltimore, Maryland, USA, 2018.

[78] F. Giannakas, G. Kambourakis and S. Gritzalis, " CyberAware: A mobile game-based app for cybersecurity education and awareness," in *International Conference on Interactive Mobile Communication Technologies and Learning (IMCL)*, Thessaloniki, Greece, 2015.

[79] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong and E. Nunge, "Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches

People Not to Fall for Phish," in *3rd Symposium on Usable Privacy and Security (SOUPS '07)*, Pittsburgh, Pennsylvania, USA, 2007.

[80] J. Smed, T. Suovuo, N. Trygg and P. Skult, Lecture Notes on Interactive Storytelling, 2019.

[81] F. Aloul, S. Zahidi and W. El-Hajj, "Two Factor Authentication Using Mobile Phones," in *IEEE/ACS International Conference on Computer Systems and Applications*, Rabat, Morocco, 2009.

[82] A. Davis, "To dock or not to dock, that is the question: Using laptop docking stations as hardware-based attack platforms," NCC Group, 2013.