CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Department of Security Studies

Master's Thesis

2024 **Brunagel Adèle**

Charles University

Faculty of Social Sciences

Institute of Political Studies

Department of Security Studies

Cybersecurity awareness & games

How to lower the human risk?

Master's Thesis

Name: Brunagel Adèle

Academic Advisor: PhD. Erkomachvili David

Study Programme: M.I.S.S - Security, Technology and Society

Year of Submission: 2024

Abstract (english):

This master's thesis delves into the topic of cybersecurity awareness and how to enhance it. It highlights the gamified alternative as a solution to the limits of the traditional methods. Hence it aims to provide an answer to the research question: Which type of gamified solution is the most effective to raise cyber awareness? To answer this question, 4 gamified tools and one traditional tool were tested by participants. Using a semi-experimental design and surveys to collect quantitative data from participants' feedback, the results were assessed under the umbrella of the constructivist learning theory. This research concludes that gamification and serious games represent a relevant alternative. The escape game was found to be the most effective method tested among the 4 others. Nevertheless, all the tested solutions presented strengths and weaknesses and had globally positive results, including the more traditional tool. Hence, a 360° strategy is proposed in the discussion section in order to combine traditional and gamified methods to achieve strong long-term effects.

Abstract (czech):

Tato diplomová práce se zabývá tématem povědomí o kybernetické bezpečnosti a jak ho zvýšit. Zdůrazňuje gamifikovanou alternativu jako řešení limitů tradičních metod. Cílem je tedy odpovědět na výzkumnou otázku: Který typ gamifikovaného řešení je nejúčinnější pro zvýšení povědomí o kybernetické bezpečnosti? K zodpovězení této otázky byly účastníky testovány 4 gamifikované nástroje a jeden tradiční nástroj. Pomocí semiexperimentálního designu a dotazníků pro sběr kvantitativních dat z reakcí účastníků byly výsledky hodnoceny v rámci konstruktivistické teorie učení. Tento výzkum dospěl k závěru, že gamifikace a vážné hry představují relevantní alternativu. Bylo zjištěno, že úniková hra je nejúčinnější metodou testovanou mezi čtyřmi dalšími. Nicméně všechny testované řešení měly své silné a slabé stránky a dosáhly globálně pozitivních výsledků, včetně tradičního nástroje. V diskusní části je proto navržena 360° strategie, která kombinuje tradiční a gamifikované metody k dosažení silných dlouhodobých efektů.

Declaration

1. I hereby declare that I have compiled this thesis using the listed literature and resources only.
2. I hereby declare that my thesis has not been used to gain any other academic title.
3. I fully agree to my work being used for study and scientific purposes.

In Paris on 29/07/2024 Adèle Brunagel

References

BRUNAGEL, Adèle. *Cybersecurity awareness & games: how to lower the human risks?* Paris, 2024. 79 pages. Master's thesis (Mgr.). Charles University, Faculty of Social Sciences, Institute of Political Science. Department of Security Studies. Supervisor Prof. PhD. Erkomachvili David.

Length of the thesis: 151.507 characters with space

Acknowledgments

First and foremost, I would like to thank my thesis supervisor, professor PhD. Erkomachvili David, whose course on cybersecurity confirmed my interest in this subject. I also appreciate his prompt, complete responses and insightful feedback on my topic. I am grateful for his trust, especially when I had to change my topic at the beginning of the year.

Additionally, in the context of my internship, I would like to thank several people. Firstly, my manager, who trusted me and gave me the opportunity to conduct this study internally. Her expertise and comments greatly assisted me in my work, along with her encouragement. Although it was an intense six months alternating between my internship and thesis, she and my colleagues helped me stay strong. Their support, kindness, and motivation pushed me to my limits, even in the toughest moments. Thanks to Florence but also Côme, Mohammed, Yassin, Max, Aurélien, Manon, Hassib, Rose, Nicolas, Lucas and of course Ornella and Anass.

Moreover, I would like to thank my loved ones, my family who also encouraged me despite the distance between us.

Lastly, I have a special thought for my fellow master's students. Together, we managed to support each other and stay strong despite the distance and the different paths each of us took. This thesis is the culmination of two years in Prague, filled with enriching encounters and experiences. Thanks to Salomé, Zoé, Margot, Martina, Jeanne, Jules, Jaklin, Massimiliano, Efe, etc…

Table of content

Introduction

Political satire and North Korean interference: Sony Pictures' 2014 cyber attack and the importance of the human link

In 2014, "The Interview" was released in theaters. The movie follows the main protagonist, Dave Skylark, an American talk show host who gets the opportunity to interview the dictator, Kim Jong-Un, who is a fan of him. Produced by Seth Rogen and Evan Goldberg, the film is described as a political satire, using comedy to critique the North Korean regime and its leader, Kim Jong Un. Upon its release announcement, several theaters chose not to screen the film due to (terrorist) threats against those who "dared" to screen it. The threat messages received stated for instance:

"*We will clearly show it to you at the very time and places 'The Interview' will be shown, [...] including the premiere, how bitter fate those who seek fun in terror should be doomed to. [...] Remember the 11th of September 2001. We recommend you keep yourself distant from the places at that time*." (Rob, 2021).

Despite these threats, the film was eventually released in theaters, with a few months delay. Although no attacks occurred in cinemas, the distribution group, Sony Pictures Releasing, fell victim to a critical cyberattack. Considered by cybersecurity experts as a "major national security issue for the United States" (Alvarez, 2014) the cyberattack took place on November 24, 2014. Conducted by a group named "Guardians of Peace," this sophisticated attack aimed to cripple Sony's computer system and steal numerous confidential and non-confidential pieces of information. Around 100 terabytes were stolen. It represents approximately the total volume of data traffic on the Internet in 1993 (Paquay, 2021). As it is often the case, identifying the attackers and their origin is challenging. However, according to an FBI investigation, North Korea seems to be behind the attack (FBI, 2014). To conduct their operations, members of "Guardians of Peace" are believed to have exploited human vulnerabilities by sending phishing emails. These emails typically contain attachments, hyperlinks, or other tools that enable the unintentional and unconscious download of malicious software (Rieß-Marchive, 2015). Through this method, the hackers could have facilitated the infection of the information system with their malware. According to an investigation conducted by WikiLeaks (2015), several phishing emails were indeed discovered. The attackers pretended to be Apple in order to obtain the Apple ID credentials from Sony Pictures employees. Since many people used the same password across multiple platforms, the attackers also attempted to use these credentials to access other accounts belonging to the victims. This investigation also highlighted Sony Pictures' very limited security culture. For instance, more than 2300 accounts had "*password*" as their password, one

of the most used passwords over the world (Rieß-Marchive, 2015). As Guy Levy-Yurista[1] argued, "the weakest link in any security system is always the human being." (Makdech & Bernard, 2014). No matter how secure a system is, if the people behind it are not trained or aware, the system remains vulnerable. The cyberattack on Sony Pictures underscored the importance of cybersecurity in our world today and its impact on international security. In this case, a nation attempted to censor a cinematic work. This attack nowadays resonates with the current climate of increasing tensions. With the war in Ukraine in addition to the rise of explosive tensions between, for instance, Palestine and Israel or China and Taiwan, international actors appear willing to employ all means to pursue their ambitions. Thus, the cyber threat should not be underestimated. Even more when everybody has a role to play to ensure security by adopting good cybersecurity practices.

Research question and hypothesis: how to effectively raise cybersecurity awareness?

How can we raise awareness about cybersecurity issues among the general population, at the individual's scale? In organizations, when awareness campaigns are conducted, they typically take the form of so-called "traditional" training sessions. In other words, a session where employees attend a course for several hours with eventually a powerpoint. More recently, companies have started using tools such as "e-learning." This involves a platform where employees can take courses individually from their computers. However, these "traditional" methods seem to struggle to impact employees' behavior (Gwenhure & Rahayu, 2024). For most people, attending these sessions or completing the training modules is more of a "boring" and "time-consuming" task they are somewhat compelled to do (Rieff, 2018). Thus, despite the implementation of these methods, most employees do not change their behavior regardless of the importance of the issues at hand. It is in this pursuit of finding a solution and an alternative that gamification and serious games come into play.

Having become a popular subject of study, these two methods, which partially or fully incorporate elements typically belonging to the world of games, are asserted as relevant alternatives to revitalize and enhance cybersecurity awareness sessions. As many studies already addressed the question of the effectiveness of gamified solutions, it will not be the primary focus of this research. This issue will be addressed in the literature review, the final objective is to explore the following question: **Which type of gamified solution is the most effective to raise cyber awareness?** Several types of gamified solutions exist, such as escape games, board games, or even gamified e-learning, but which one could be the most effective? Which one could ensure strong motivation, learning and convince participants to change their behavior? This master's thesis will seek to answer this question. To do so, three types of solutions will be compared through a semi-experimental research: board game, e-learning platforms and escape game.

[1] Chief Executive Officer at Synthace & Expert in Cyber Security issues

Summary and organization of the Master's thesis

This research is structured in six main parts in addition to a conclusion. The first section addresses the contextualisation of the topic by exploring the key concepts. On the one hand, cyberspace, its security, actors and challenges. On the other hand, the concepts of gamification and serious games. Secondly, the theoretical framework section will highlight the relevance of the topic and the theory selected to analyze the results, namely: the constructivist learning theory. Thirdly, the methodology part frames the research design, the methods used in data collection and analysis, the validity, reliability and ethical consideration in addition to the limits of this quantitative research. The fourth part presents a literature review on the efficacy of traditional and gamified solutions. It is followed by the findings section. This part stresses the results of the research which underline the escape game and the ultra-gamified solutions as the "most effective", not without certain constraints. The discussion, the last section, brings explanations and recommendations based on the results. Finally, the conclusion summarizes the whole research and opens the topic to security discussion and perspectives to further consider.

Contextualisation: Defining the key concepts

Introduction

Before diving into the research, the main and key concepts must be clarified, namely cybersecurity and two gamified concepts: serious games & gamification. Therefore, both concepts will be contextualized, defined and explained in order to highlight their relevance, importance and challenges. Hence, this section will firstly discuss cyberspace in order to reveal the importance of cybersecurity in international security and the key role that humans play. Then, in a second part, gamification and serious games will be discussed in a general perspective but also in the context of education and awareness. In other words, this section set the foundation to develop the rest of this research.

1. Cyberspace, cyberattacks and cybersecurity: an overview

Cyber-related concepts are rather popular nowadays, but the meaning behind cyberspace, cyberattacks and cybersecurity remains quite blurry. Hence, this first section aims to provide a comprehensive overview of cyberspace, cyberattacks, and cybersecurity. Firstly, the concept of cyberspace will be discussed in order to contextualize this research. Secondly, cyberattacks will be addressed, including the actors, the challenges and consequences. Thirdly, the matter of security inside this new realm will be explored. This section seeks to set up an overview for understanding the broader context in which cybersecurity awareness and gamification initiatives are situated.

a. Cyberspace: origins, definition and its structure

Cyber is such a perfect prefix. Because nobody has any idea what it means, it can be grafted onto any old word to make it seem new, cool — and therefore strange, spooky.
- New York Times, 1996 (Online Etymology Dictionary)

The definition(s) of cyberspace

In the 80s and 90s, the use of the prefix ‘cyber’ became increasingly popular. More and more words were made up from it, such as cyberpunk, cyberspace, cybercafé, cybernauts, cyborgs, cybernation… It’s in 1984, that “cyberspace” was mentioned for the first time, in a book called “Neuromancer”. In this science-fiction novel written by William Gibson, the author defined cyberspace as "the online world of computer networks and especially the Internet, the environment in which communication over computer networks occurs” (Featherly, 2024). Initially considered as a “buzzword” and despite its origins in science fiction, the concept of cyberspace is widely used and accepted, including by scientists and scholars. If William Gibson’s definition proposes a first insight of what could mean

cyberspace, some scholars would argue that it should be defined as "an operational domain framed by use of electronics to exploit information via interconnected systems and their associated infrastructure" (Clark et al. 2014). Others, that it should be referred to as "the artifacts based on or dependent on computing and communications technology; the information that these artifacts use, store, handle, or process; and how these various elements are connected." From a more institutionalized perspective, the National Institute of Standards and Technology (NIST), a reference in cybersecurity, defined cyberspace as "a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." (NIST SP 800-39). At last, these definitions share strong similarities and highlight with more or less details what cyberspace is. In addition, as argued by de Bruijn & Janssen (2018) most scholars generally share a similar understanding of what represents cyberspace.

For the rest of this research, the definition proposed by NIST will be used as a reference for the following reasons. First, NIST is a benchmark in terms of cybersecurity. The Institute has published numerous high-quality cybersecurity frameworks that are used by companies and also serve as sources of inspiration. Moreover, their definition has the advantage of highlighting several important aspects of cyberspace, particularly its multidimensional perspective. While cyberspace is often instinctively associated with the internet, notably for its interconnectivity, it should not be limited to that (e.g., the telegraph also enhanced interconnectivity, but cyberspace is more than just interconnectivity). Cyberspace is also an ecosystem composed of diverse actors with varying degrees of competition. Created and sustained by man, the user factor must be included inside the definition of cyberspace. To fully understand this, it is possible to deconstruct cyberspace into multiple layers. This allows for a better understanding of its functioning and how its different components are interconnected.

The (de) construction of cyberspace

In order to better understand how cyberspace works, Choucri & Clark proposed in their book *International relations in the Cyber Age: the co-evolution dilemma* (2019, 33-65.), a four-layer model of cyberspace. Other models based on more or fewer layers also exist, offering varying levels of details. The four highlighted layers in their book, from bottom to top, are: "the physical foundations (1), the platform layers (2), the information (3), and the people (4)". As it is represented in figure 1, every layer is related, built on each other.

The (bottom) **physical layer** (1), includes all the physical devices on which the internet is built. Hence, it's about all the electronic and computer components, the servers, the networks… It also includes all the elements enabling communications channels such as wires, fibers, satellites, radio waves, etc… In other words, this layer is about all the tangible elements situated around the world.

This physical condition implies a physical location around the world, and thus, makes the components come under specific jurisdiction depending on where they are geographically based, unlike other layers. The **platform layer** (2) is about providing "the services that realize the structure of cyberspace". Divided in three parts: internet, services and application, they are all enabling the below layer information. For instance, for the web to function, it requires the two lower layers, namely, specific services as well as the operation of the internet. Conversely, DNS (services) cannot work without the internet. Thirdly, the **information layer** (3) is also at the core of cyberspace. It can take many shapes for different purposes. For example, information could be videos, photos, web pages, an online book…It includes the "creation, capture, storage and processing of information and content". Finally, the last layer (4) is structured around the people, **the users**. They are the actors, the ones who directly or indirectly shape cyberspace. For instance, Wikipedia only exists because people want to participate in Wikipedia. In other words, the four layers are interconnected, interdependent but also follow a hierarchy. Each layer relies on the one upon which it is built. Yet, some layers have physical aspects and thus have to follow the rules of the physical world such as legislation, potential natural disaster, or physical restrictions and limitations imposed by physics' laws. However, when it comes to the intangible side of cyberspace, legislation and sovereignty are harder to impose which leads to great debate, notably about states' sovereignty. Although cyberspace is forged by humans, it happens to also escape their control.

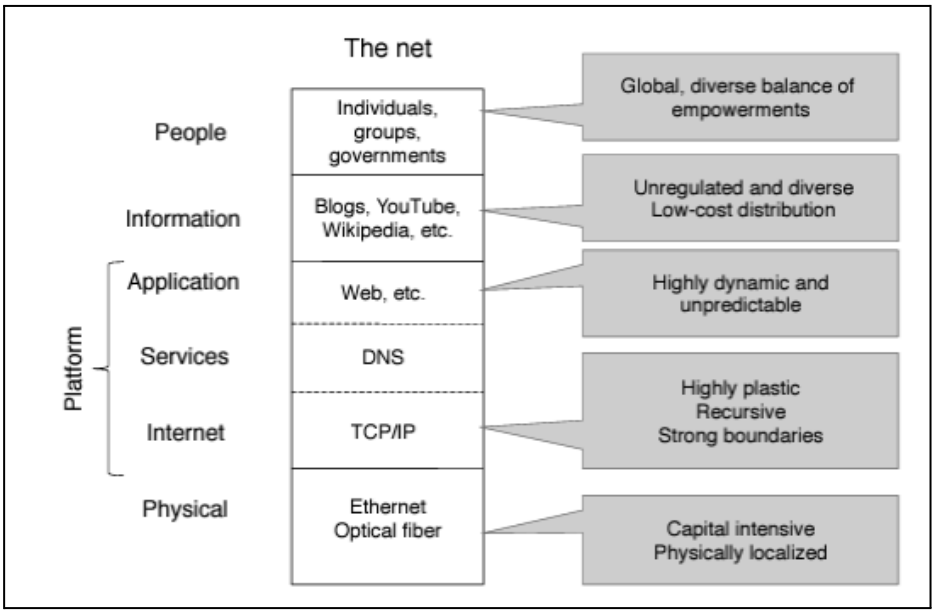

Figure 1: Representation of the net and its main characteristics
Source: *Chourci & Clark, 2018*

Therefore, despite origins in science fiction, "cyberspace," is anchored in our reality. Several definitions exist, sometimes too wide, too narrow or too politically-oriented… The NIST's conception

of it captures the main features and elements at the core of cyberspace. Exploring the layers of cyberspace highlights key elements, especially regarding the importance and the role of humans in its functioning.

b. Cyberattacks: definition, actors and consequences

"Major cyber-attacks are, [...] a matter of 'when, not if'" argued Ciaran Martin in an article in The Guardian (MacAskill, 2018). States, small or big companies, individuals… Everybody is at risk when it comes to cyberattacks. As claimed by the former head of the UK's National Cyber Security Center, cyberattacks will happen, it is just a matter of time before they occur. By 2025, it is estimated that cybercrime will cost around $10.5 trillion per year (Morgan, 2022). Increasingly frequent, these attacks are costly and often have serious consequences. When it comes to the definition of "cyberattack", just as with cyberspace, no generally accepted definition exists. Hence, cyberattack can be understood and defined differently. Depending on the context and the geographic location, the definition can be quite different, more in harmony with the political ideology of certain states (Saalman et al. 2022. This factor will not be explored in this research, as it does not bring valuable insight to answer the research question stated in the introduction. Therefore, the aim is to examine the definitions of a cyber attack from a Western perspective.

According to IBM[2], one of the leading companies in the global computer industry, a cyberattack refers to "any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device" (IBM). This definition proposed by IBM remains rather broad and inclusive. It summarizes the "unofficial" consensus on what is generally meant by a "cyberattack." However, some scholars prefer to differentiate between two concepts conflated in this definition: on one hand, the concept of a 'cyberattack', and on the other, 'cyber exploitation'. In this case, we tend to speak of a cyberattack when it involves "an action intended to cause a denial of service (DoS) or damage to or destruction of information stored in or transiting through an information technology system or network." While the aim of a DoS is to "render a properly functioning system or network unavailable for normal use", a damaging attack will seek, for instance, to "alter a computer's programming" and change its behavior. It can even result in the physical destruction or blockage of electronic components (Clark et al. 2014, p. 32). Conversely, we refer to a "cyber exploitation" when the purpose of the operation is to "exfiltrate digitally stored information that should be kept away from unauthorized parties that should not have access to it" (Clark et al. 2014, p. 31). Thus, on one hand a cyberattack will target the electronic component, the proper functioning of systems, etc… while on the other hand, cyber exploitation will seek (unauthorized) access to information.

To sum up, this distinction highlights the dual nature of operations in cyberspace. It involves both

[2] International Business Machines (Corporation)

harming and destabilizing, as well as stealing and manipulating. For the remainder of this thesis, when the concept of a cyberattack is discussed, it will implicitly include the notion of cyber exploitation. In other words, it will refer to the broad and comprehensive understanding of this concept, as defined by IBM.

The hostile actors in cyberspace

Behind malicious operations in cyberspace is a diverse array of actors with varying motivations and capabilities. This section will examine and explore the major categories of hostile actors which operate in cyberspace, and what differentiates them.

Firstly, as detailed in the previous part, a cyberattack[3] is the result of an "adversarial (or hostile) cyber operation". The **actors** (1) behind such operations can either act *alone* on their own, act as *independent groups* or be *sponsored by states*. They can also be part of *organized crime* or *transnational terrorism*. Such variety in the profiles can be explained with the low entry cost to lead operations. Secondly, when it comes to the motivations (2), some are only following their *curiosity*, *testing* their *skills* and *limits*. Others, to satisfy their *ego* or for the *thrill*, will seek to penetrate or vandalize networks or systems that are sensitive or reputed as highly secure. Of course, some actors are also driven by *profit*. They might steal information to resell it, demand ransoms, or, for example, offer their services as mercenaries. Moreover, some actors could also be motivated by an *ideology* or some "nationalistic considerations". These impulsions might be coupled and can evolve through time for individual actors and groups. Finally, one last criteria concerns the **skills and knowledge** (3). Not all actors represent the same threat and thus the same level of risks and protection. From the knowledge perspectives, they can be divided into *three categories*. The first part concerns players with a relatively low level of technical expertise (a). They have a "rudimentary understanding" and thus they rely on tools that were created by others to conduct their operations. Secondly, actors with "intermediate" skills (b) are the ones capable of developing their own "hacking tools". Thirdly and finally, the ones with the most advanced level (c) represent the highest threat. In other words, they have the capacity to find breaches and weaknesses, they can create tools that other hostile actors could use. Consequently, they can deploy sophisticated attacks which often require huge resources, including time and participants. Most of the time, they are sponsored by states and therefore can be identified as Advanced Persistent Threat (APT). The support of states or other powerful groups provide the experienced actors with resources, both financially (salary, material, logistics) and in terms of knowledge (Clark et al. 2014; Choucri & Clark, 2018).

[3] It also includes cyber exploitation as argued in the previous part.

The threats and their consequences

According to IBM, the average cost of a data breach is $4.45 million (IBM). However, this cost can be much higher. Cyberattacks are expensive and have been steadily increasing over the years (IBM). To carry out a cyberattacks[4], hackers can employ various methods. They often exploit vulnerabilities in information systems and networks or may attempt to trap users. But the finality of these attacks can vary. In connection with what was discussed in the previous part, an hostile operation will generally seek to target at least one of the three pillars of security of an Information System (IS), namely: **confidentiality, availability, and integrity** (CIA). Firstly, when an attack aims for confidentiality (1), the goal is to gain access to restricted data. For instance, when intruders steal confidential information, confidentiality is at risk. Secondly, if the objective of an operation is the availability (2), it means that the attackers want to limit (partially or completely) the owners' access to their data. When a company is the victim of ransomware, usually, all its data is blocked (crypted), and thus unavailable until the ransom is paid. Thirdly, attackers may also target data integrity (3) by altering or manipulating the information present on an infected system or network. In this case an hostile actor could for example change the bank information of a company in order to redirect wire transfer to another account (Hakmeh et al. 2022). These three criterias (CIA) are also used as “protection goals” for the security of an Information System (IS). Sometimes, a fourth criteria can be added, namely: “authenticity”. It refers to the requirement to have authentified (confirmed identity) the users before they can have access to specific data such as confidential files, mails, applications … This last criteria overlap or can be mixed to some extent with integrity of authenticity. For example, a hacker could use the lack of MFA (Multi-Factor Authentication) or poorly secure authenticity factors to have access to documents, accounts, etc… (Reffgen, 2018, Chourci & Clark, 2018).

There are many types of cyberattacks and consequently, different consequences. Several major categories of operations stand out. First, cyberattacks using malicious software (1), more commonly known as "malware." These software can take various forms with different functionalities. The most well-known examples are Trojans, ransomware, spyware, and rootkits. They can affect the operating system, destroy, steal, or corrupt data and files on the infected computer or network. Secondly, social engineering operations (2) primarily target humans. These operations manipulate victims into performing actions they shouldn't, such as sharing confidential information, downloading files, clicking on malicious links, or sending money. To achieve this, attackers are well-versed in human vulnerabilities and may use various means of pressure or deception. Phishing is widespread and is one of the most common cyberattacks globally. According to Interpol, “cyberattacks such as phishing may be borderless and virtual in nature, but their impact on victims is real and devastating.” It is estimated that 90% of successful cyberattacks begin with a phishing email (Dzuba & Cash, 2023). This type of attack is easily deployable, requiring little preparation time and minimal financial or human resources.

[4] As argued in the previous part, here cyberattacks include cyber exploitation.

Thirdly, the (Distributed) Denial of Service (3) (DDoS) seeks to overwhelm the resources of a system. Consequently, the system cannot adequately perform. It can be done using one (DoS) or several (DDoS) sources to generate the requests paralyzing the targeted system. Finally, there are also other types of attacks that we will not delve into but can be mentioned, such as man-in-the-middle attacks, supply chain attacks, SQL injections, zero-day exploits, etc…

c. What is cybersecurity?

In the early 1990s, as the use of computers was spreading worldwide, especially among individuals and businesses, the "Computer Science and Telecommunication Board" (CSTB[5]) was already publishing "Computers at Risk," an alarming report about the dissemination and increasing use of computers. According to the Board, "as computer systems become more prevalent, sophisticated, embedded in physical processes, and interconnected, society becomes more vulnerable to poor system design and attacks on computer systems". Thus, the CSTB was already warning about the dramatic changes in "the nature and magnitude of computer system problems". They also argued that "known techniques are not being used" when it comes to increasing cybersecurity, which some scholars or cybersecurity experts might still agree with (Clark & Berson, 2014). Hence, issues related to computers and by extension, cyberspace, are an inherent feature. Warnings about how the world could become with such technologies and innovations were already rising. This growing risk, which began to raise alarms in the 1990s, has been confirmed and amplified over the years. In response to these risks, partially discussed in the previous section, it is essential to implement appropriate security measures, known as "cybersecurity." According to Ani et al (2016, p.170) 'cybersecurity' can be defined as the "harmonization of capabilities in people, processes and technologies; to secure and control both authorized and/or unlawful access disruption or destruction of electronic, computing systems (hardware, software and networks), the data and information they hold". The aim is to protect the technologies such as computers, hardware, software, networds, or data from potential criminals or hackers.

To ensure cybersecurity, three features are often mentioned by scholars. Also called the "triad of cybersecurity" it includes the "people", the "processes" and finally, "technologies" (Clark & Berson, 2014). Properly "aligning" these three components is crucial for the cybersecurity of organizations. This triad underscores that effective cybersecurity strategy is not solely relying on advanced technological solutions but also requires robust processes and a well-informed and vigilant workforce (Rieff, 2018). In his article, Howarth (2014) points out that many current approaches focus primarily on technological solutions, often neglecting the critical roles of people and processes. This oversight can lead to gaps in cybersecurity, as technological defenses alone are insufficient without the support of well-defined processes and an educated, aware workforce. A PWC's report indicates that a

[5] Established in 1986

substantial percentage of security breaches are attributed to human error. For instance, in 2013, 36% of the worst security breaches were caused by human mistakes, and in 2015, 31% were initiated by human errors, with an additional 20% resulting from intentional misuse of systems (PWC, 2016). Hence, as highlighted in the theoretical section, humans are one of the three main keys to ensure cybersecurity. Also considered as the "weakest link" of the chain, humans are the vulnerability factor that cannot be controlled just as an Information System would be for instance. People make mistakes, on purpose or not, they can be influenced, in other words, people can be unpredictable. To limit human error, cybersecurity awareness and adequate training are critical components of a cybersecurity strategy.

To conclude, this first part addressed the concepts of cyberspace and its main related issues and concepts such as cyberattacks, cyber actors, cyberthreat and consequently, cybersecurity. It began by tracing the history and various interpretations of cyberspace and ultimately settled on the multidimensional perspective provided by the NIST framework. Secondly, cyberattacks were defined and addressed. The different actors involved were approached, so were their motivations, and specificities. Thus, the major threats and consequences of cyberattacks, including breaches of confidentiality, availability, and integrity of information systems were presented. Finally, the need for a comprehensive cybersecurity strategy that integrates people, processes, and technologies was underscored as a necessity to effectively protect against cyber threats.

2. Gamification and serious games

Over the last few years, the concept of integrating game elements into non-game contexts has attracted significant attention, leading to the development of two closely related concepts: gamification and serious games. This second section aims to delve into the fundamental aspects of these concepts. Firstly, the link between humans and games will be addressed, followed by two sections focusing on, on the one hand, gamification, and on the other hand, serious games. Their definition and origins will be discussed. To sum up, this part aims to provide insights about serious games and gamification, the two additional concepts at the core of this research.

a. Humans & Games: an inherent relation?

"Games are a crucial aspect of human culture and society and promote motivation and engagement" argued Krath et al. in their article about gamification (2021). A "game" refers to a "structured play with rules, goals and challenges for the purpose of entertainment". Throughout history, it indeed seems that games are an inherent part of all societies, since almost forever. For example, the earliest known dice was found in Iran and dates back 3,000 years. Additionally, the first game with an

educational purpose, the "Mancala," was used around 1400 BC. It was regarded as an "accounting tool for trading animals and food." (Laamarti et al. 2014).

However, “game” should not be confused with “play”. The distinction is crucial for understanding the dynamics of ludic activities. Games are structured activities with explicit rules, clear objectives, and often a competitive element (ludus). In contrast, play is a broader and more flexible category characterized by free and creative improvisation without rigid constraints (paidia). Both gamification and serious games focus on this side (game). The main difference is that Serious games are a “whole” game while gamification uses “parts” of games[6] as described in figure 2. This will be more developed in the next sections.

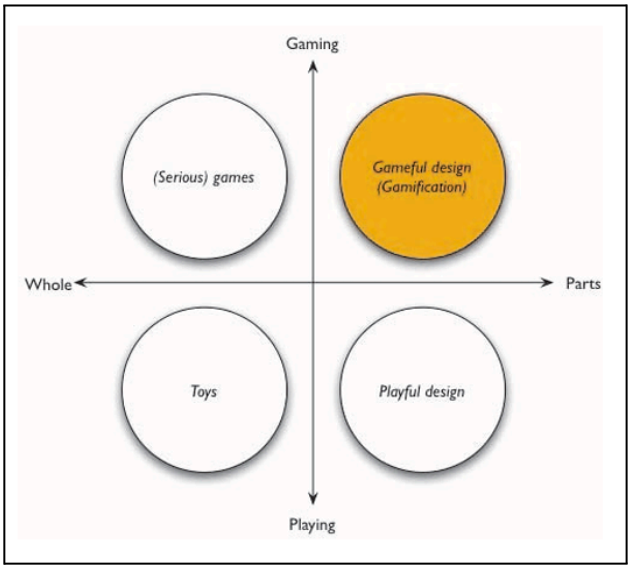

Figure 2: Serious games & gamification, “between game and play, whole and parts”
Source: Deterding et al. 2011

b. Serious Game: definition and history

Serious game: the origins

If literature, cinema, and art can convey messages and teachings, why not games? This claim is not new and did not emerge solely in the modern era as argued earlier (cf: Mancala). However, the use of games for educational purposes saw significant development during the 20th century. For instance, the American military started to use "wargames" during World War II to improve their reputation among the population (Laamarti et al. 2014). Nevertheless, it was in 1970, with the publication of the book *Serious Games* by Clark Abt[7], that the theoretical foundations of serious games as we know them today were established. In this book, Abt describes serious games as having "an explicit and carefully thought-out educational purpose and are not intended to be played primarily for amusement”. More recently, it is still possible to witness a growing interest in this topic. Though it has been increasingly studied academically since the 90s, Laamarti et al., in their article (2014), highlighted a particularly pronounced rise in the early 2000s, with a notable surge beginning in 2010. Moreover, beyond its growing appeal to scholars, serious games are also popular in the industry. Its use in businesses remained relatively low in the 1990s before surging in the early 2000s. Thus, by only referring to the

[6] Both concepts will be further discussed in the following partS.
[7] American Scholar and Scientists. He is originally from Germany.

evolution of the market, serious games seem to be appealing and demanded by companies and organizations.

Serious game: definition

A serious game serves as the foundation for game-based learning. The latter can be understood as the "achievement of defined learning outcomes through game content and play and enhancing learning by involving problem solving spaces and challenges that provides learners [...] with a sense of achievement." (Krath et al. 2021, p.2) Thus, the result of this "achievement" is a "serious game". Several definitions of a serious game exist, depending on the industries and their needs. In general terms, a serious game is a game which has as its primary purpose: "education". For example, a serious game can take the form of a board game, an escape game, a wargame, a simulation, a video game, etc… However, it is also important to note that numerous recent studies consider video games to be the main form of serious games. This is exemplified in articles written by Mouaheb et al. (2012), Ullah et al. (2022), and Belotti et al. (2013) or Houda et al. (2012). Consequently, a significant majority of publications focus solely on the subject of serious games predominantly concentrate on video games rather than on the other previously mentioned models. Nevertheless, for the continuation of this research and in order to align with its purpose, the concept of serious games will not be limited to the video game format.

c. Gamification or gamifications?: a contested concept

One or several gamifications ?

Sometimes confused with other designations such as, "funware", "game layer", "applied game" or "productivity game", gamification is most of the time defined as "the use of game design elements in non-game contexts" (Deterding et al. 2011, pp.9-10). It is perceived as "a process of enhancing services with (motivational) affordances in order to invoke gameful experiences and further behavioral outcome." (Hamari et al., 2014). As previously discussed, gamification seeks "game" and not "play". The aim is to enhance a "service" with gameful elements. These features related to games can be identified from different perspectives. It could be seen, very widely and from a "liberal perspective", as any elements present in games. Deterding et al., proposed to limit these elements to the one that are "characteristics to games" or the more recurrent (2011). Hence, a non-exhaustive list of gameful elements can include, avatars, ranks, quests, levels, teams, limited time, etc …

Origins and (contested) popularity

The concept of gamification is rather new. It firstly appeared in literature around 2008 inside the "digital media industry". However, it's only around 2015 that "gamification" really started to spread (Deterding et al. 2011). A study by J. Hamari et al. (2014) examined the evolution of

gamification-related publications on Google Scholar and Scopus[8], revealing a significant increase in the number of publications between 2010 and 2013. As shown in Figure 3, in 2010, fewer than one hundred publications were recorded for the entire year on Google Scholar. Three years later, in 2013, the number of publications rose around 200 per month throughout the year, both on Google Scholar and Scopus. (Hamari et al. 2014).

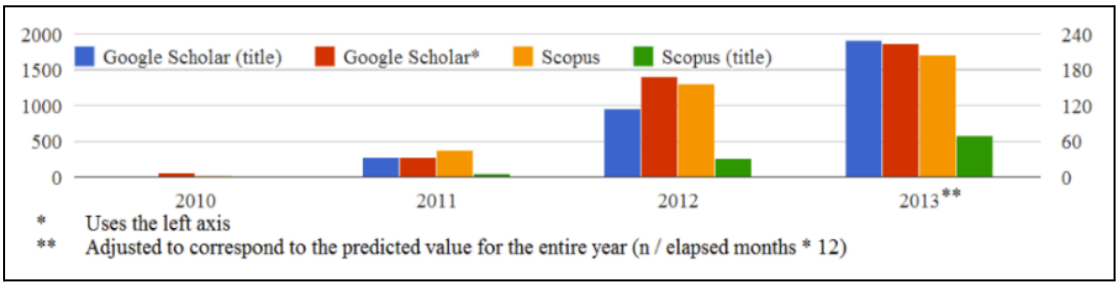

Figure 3: "Evolution of publication paper related to 'gamification'"

Source: Hamari et al. 2014

Despite this significant increase, which demonstrates a growing interest in this concept, gamification is not universally accepted. In an article published in *The Atlantic* (2011), Ian Bogost[9] stated, 'gamification is bullshit' (Landers et al, 2018). Supported by Jan Klabbers[10], who also characterized gamification as "exploitationware". For its detractors, gamification is merely a marketing term, created to cater to a commercial practice with the sole aim of selling more. However, for its proponents, this argument is unfounded and reductive, as defended by Landers et al. (2018). To them, limiting gamification to a sales strategy is an "oversimplification". In their article "Gamification Science, Its History and Future" (2018), the authors highlighted several counter arguments against Klabbers and Bogost's claim. Firstly, the lack of empirical evidence (1) to support their argument. Conversely, academic articles and studies supporting the utility of gamification and the credibility of 'game science' are increasingly prevalent. When the article was written in 2018, the authors identified over 30,000 publications solely on Google Scholar. Secondly, there is a 'misinterpretation' of what gamification actually is (2). As the authors highlighted in their article, "gamification is not itself a product; one does not create a gamification as one creates a game." Although several definitions of gamification exist, the concept remains intrinsically "a design process [...] intended to augment or alter an existing real-world process using lessons (initially) from the game design research literature to create a revised version of that process that users will experience as game-like" (p. 317). Thus, it can be applied in various contexts such as marketing but also education, health care, fitness… Finally, gamification is a "legitimate scholarly enterprise" (3). Several frameworks and studies seek to determine the effects and boundaries of the concept as it will be discussed further in this research.

[8] Google Scholar and Scopus are 2 specialized search engines for academic publications
[9] Video Game designer and scholar (Washington University in St Louis)
[10] Dutch Academy Professor (University of Helsinki)

Gamification science aligns with post-positivism as it emphasizes empirical evidence, but also acknowledges the existence of subjective interpretation in order to fully capture the effectiveness of the concept. (pp. 316-318).

To conclude, this section examined gamification and serious games, focusing on their definitions, origins, and distinctions. While serious games were defined as educational tools that encompass various formats, not limited to video games, gamification can be referred to as the use of game design elements in non-game contexts. Moreover, this second subsection highlighted the fundamental role of games in human culture and clarified the difference between games and play.

Conclusion

To conclude, this contextualisation section brought clarification and the foundation for the rest of the research by exploring the essential concepts of cybersecurity and the gamified concepts of serious games and gamification. The first part focused on cyberspace, detailing its history, definitions, and the critical role of cybersecurity. On the one hand, it addressed the nature of cyberattacks, the actors involved, their motivations, and the significant threats posed to information systems. On the other hand, it underscored the necessity of a comprehensive cybersecurity strategy integrating people, processes, and technologies. The second part explored gamification and serious games, defining and distinguishing them while emphasizing their educational applications. It also highlighted the intrinsic connection between humans and games. Therefore, this contextualisation provides the foundational understanding necessary to advance the research.

Theoretical Framework: how to evaluate the efficacy of gamified solutions?

Introduction

The purpose of this section is to complete the theoretical basis and the context of the research. It brings additional contextualisation regarding the theories regarding the topic of gamification and serious games. Consequently, the theoretical framework can be considered as an analytical lens for interpreting the findings of this research. This section is divided into 3 parts. The first one is about the relevance of the main topic of this research: the importance of human awareness regarding cybersecurity good practices. The second part proposes a review of theoretical frameworks in order to have an overview of the theories used to understand gamification and serious games. Finally, the third and last part presents the theories selected for the rest of this research. The aim of the last section is to set a theoretical basis that can be used to build, analyze and understand the results of the experiment developed in the methodology part.

1. Humans and ensuring cybersecurity: relevance, prospects and justification

In 2002, The Economist published an article titled “The Weakest Link: If Only Computer Security Did Not Have to Involve People.” Around the same time, Kevin Mitnick (Greene, 2000), a former American hacker convicted of multiple high-profile hacks, argued that, "companies spend millions of dollars on firewalls, encryption, and secure access devices, and it's money wasted; none of these measures address the weakest link in the security chain [the people]." This observation is still shared by cybersecurity experts; the human factor is often the entry point that allows hackers to launch their operations. Why are there human vulnerabilities? What are the consequences? This section aims to answer these questions, but also to highlight the importance of this issue, and emphasize the lack of research on alternative solutions.

a. Humans as the “weakest link of the chain” of cyber security

People are generally considered as the “weakest link of the chain” when it comes to ensuring cybersecurity for several reasons. Firstly, they are more vulnerable to attacks. Secondly, most of them lack awareness and training. Finally, human nature, by itself, represents a source of threat.

Humans are vulnerable to several attacks

According to a report published by Cloudflare in 2023, it is estimated that “90% of successful cyberattacks start with phishing emails” (Duzba et Cash, 2023). This type of attack can use emails, SMS, fraudulent websites, or even phone calls to deceive their targets. The attackers' goal is to gather sensitive data or trick victims into downloading malware. Phishing attacks are frequent and their breaches cost organizations an average of $4.76 million, which is higher than the global average cost of breaches at $4.45 million (IBM). This type of attack often goes hand in hand with other methods used by cyber attackers, such as social engineering, the use of deep fakes, email account compromise, or CEO fraud. For example, in the case of CEO fraud, also known as a "Business Email Compromise (BEC)," the fraudster impersonates the highest authority of a banking institution to urgently and confidentiality request a significant transfer from an employee. This method is used to carry out illicit bank transfers (Microsoft). In all cases, attackers target human weaknesses and the potential for human error. These operations are becoming increasingly sophisticated, benefiting from the democratization of AI, making them sometimes more difficult to recognize.

Most of users lack of awareness and training

Moreover, several reports highlight the lack of cybersecurity awareness in companies. According to IBM (“Cost of Data Breach, 2020), 52% of data breaches implied human mistakes linked to poor or none cybersecurity awareness. Additionally, a MediaPRO report, “State of Privacy and Security Awareness” (2020), evaluated employees’ cybersecurity knowledge with assessment tests. The results showed that 72% of them failed the exercise. However, these results are the consequences of poorly made awareness sessions, not the lack of it. In 2022, it was estimated that around 97% of organizations were already implementing such training (ThriveDX, 2022). Thus, most people in organizations do receive cybersecurity awareness sessions, the issue might be more on how they receive this knowledge. As it will be argued in the literature review, the “traditional” ways are nowadays lacking in effectiveness. Hence, other solutions arise such as gamification and serious games.

Human nature represent a threat by itself

Finally, people de facto represent a possible source of threat. Firstly, as discussed earlier, people make mistakes. Even experts in cybersecurity happen to make mistakes, so as “regular” employees. Secondly, most users, despite training and cybersecurity awareness sessions, refuse to change their behavior and habits. For instance, using strong passwords, with the help of a password manager, and Multi-Factor Authorisation are three solutions which easily enhance the security access to accounts. Nevertheless, it is often perceived as “inconvenient” or “time consuming”. Yet, according to the 2021 Verizon Data Breach Investigations Report, 81% of data breaches related to hacking involved stolen

or weak passwords (Verizon, 2024). Finally, humans can easily be corrupted or turned against their organization for various reasons (ideology, revenge, ethics, etc.). As a result, it is possible for an employee to willingly participate in an operation aimed at harming a state or an organization by disclosing, modifying, or destroying information or other key elements of an information system.

b. Master's *Thesis and Internship*

This master's thesis is anchored in the International Security and Studies' program offered by Charles University in Prague (Czech Republic). Additionally, it is the result of a final internship at a cybersecurity consulting firm based in Paris (France). Thus, it provides an opportunity to bridge the gap between academia and professional life through a master's thesis. This research aims to connect international security needs with cybersecurity requirements by addressing real-world demands: how to lower the human risk in cybersecurity?

As discussed in previous sections, raising user's awareness regarding best practices in cybersecurity is an urgent need in a world where cyberattacks are increasingly frequent. Given this reality and the observation that current methods are either insufficient or inadequate to nowadays' needs, this thesis proposes an alternative approach to reinvigorate awareness methods.

However, while it addresses a business-need, this research is not disconnected from international security. The issues and consequences of cyberattacks already influence the international and national balance of many countries. To cite just one example, in 2022, Costa Rica was brought to its knees by a ransomware attack. Consequently, the country was paralyzed for several weeks (Burgess, 2022; Reuters, 2022). Moreover, cyberattacks are also used for war as it's the case in Ukraine or to destabilize countries (Mueller et al. 2023). Thus, this topic addresses an issue relevant to all stakeholders at various levels. Whether private companies, countries, or individuals, adopting good cybersecurity practices concerns us all.

Hence, ensuring cybersecurity without including the people is impossible. As they are the users, they can firstly be the target of cyber operations. These attacks rely on people's inherent vulnerabilities. Secondly, many employees are still lacking in cybersecurity knowledge. Consequently, they do not know how or which behavior they should adopt. Finally, the last threat is the people. Easily corrupted, unintentional mistakes, laziness, habits… the list of vulnerabilities of human nature is long and can be unpredictable or rather hard to change. Nevertheless, involving people in cybersecurity could establish a "human firewall", consequently enhancing the security and lowering the risks. To reinvigorate cybersecurity awareness, games appear to be an effective solution as it will be developed in the literature review with more details.

2. Theoretical Literature Review: Learning, Behavior and Motivation theories

Overview of the theories: the three main thematics

In the article "Revealing the theoretical basis of gamification" (2021), Krath et al. carried out a meta-review of the theoretical basis of gamified solutions. They highlighted the lack of shared theoretical foundations when it came to gamification or serious games and found that 118 theories were used with more or less popularity and frequency. Figure 4 represents the main theories and their distribution. The bigger the circle is, the more often used a theory is. The arrows between the different circles represent "explicitly mentioned inclusions of one theory into another". Thus, most research on this topic used different theories from which different results can derive. The colors refer to the three main categories and thematics at the core of the theories: "affect and motivation" (1), "behavior" (2) and "learning" (3). Finally, the "mixed-color" circles can be understood as using undistinguishable "thematic". These thematics are not to be opposed. On the contrary, most of these are complementary. Despite having different approaches, they remain interconnected.

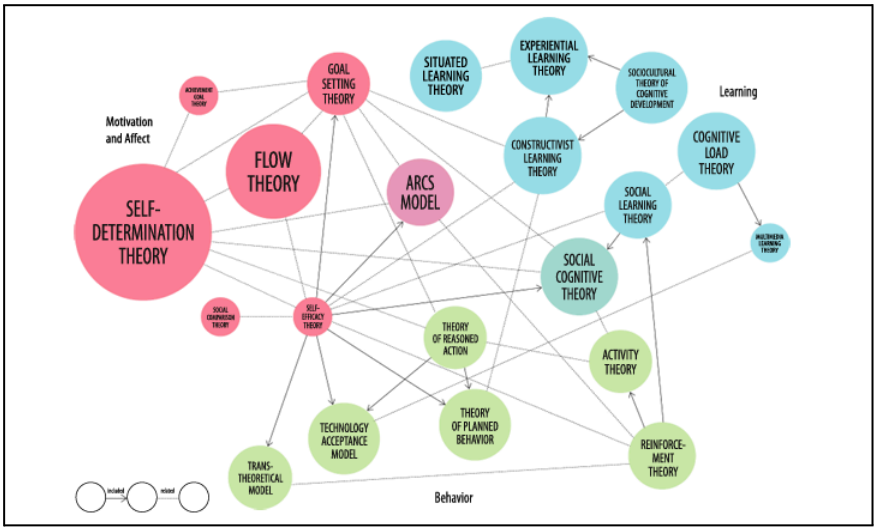

Figure 4: Overview of the theoretical landscape regarding gamification & serious games

Source: Krath et al. (2021)

The following subsections present the main theories that were used, according to Krath et al.'s meta review (2021). A brief summary with the key elements of the theories is presented. As there is a huge amount of theories, only six were selected: the self-determination theory, the self-efficacy, the theory of planned behavior, the constructivist learning theory, the social cognitive theory and the ARCS model. Each of these belongs to one or several categories developed earlier. Despite being for some the most used frameworks, they appeared to be the more relevant ones in this context. As the aim of this research is to find which type of gamified solution works the best, the theoretical framework selected must be able to propose a relevant axis of analysis. To be considered as effective, the

solutions must have an impact in the learning, the motivation and the behavior of the participants. Hence, the selected theory is linked to others from different categories. Therefore, it provides broader perspectives that could be useful for the aim of this research.

- **Motivation and affects: self-determination (SDT)**

The self-determination theory was the most frequently used theory, 82 times, according to the meta-review of Krath et al. It belongs to the category of "affect and motivations" and is closely related to almost every theory inside this thematic such as the "flow theory", the "goal setting theory", or the "self-efficacy theory". It seeks to understand how motivation works and how it can be set up regarding learning in our case. This theory has at its core the concept of "basic psychological needs". These needs must be fulfilled for the well-being of the participants. It includes three dimensions: competence, autonomy and relatedness. The "competence" refers to the need to feel effective and capable, to seek the challenges and the knowledge. The "autonomy" can be understood as the sense of freedom of choice in your own actions. Finally, "relatedness" is about the feeling of being connected and significant to other people, in other words, it's about support and encouragement. Each of these three perspectives must be operating in combination in order to be effective and motivated. To satisfy these needs, the participants have to be "proactive" in the process of learning, though they might have different reasons to "learn".
These motivations are either "intrinsic" or "extrinsic". The first one involves engaging in activities for the inherent satisfaction and pleasure they provide, which results in a high level of self-determination and autonomy. Conversely, extrinsic motivation involves engaging in activities for external rewards or to avoid negative outcomes and it influences the degree of autonomy. Different types of extrinsic motivations can be differentiated and classified on the basis of the "autonomous scale". For instance, "external regulation" is the least autonomous and is driven by external demands or rewards. Moreover, "introjected regulation" involves internal pressures such as guilt or self-approval, which indicates a moderate level of autonomy. Additionally, "identified regulation" occurs when behaviors are driven by personal goals and values that the individual identifies with, showing a higher degree of self-determination. Finally, the most autonomous form of extrinsic motivation is "integrated regulation", where behaviors are fully assimilated with the self and align with personal values and needs. According to F. Guay, "the more autonomous the motivation is, the more it should lead to positive consequences…". Thus, goal setting plays an important role in the motivation for the participants. (Guay, 2022; Krath et al. 2021)

- **Motivations and affects: the self-efficacy theory**

Less popular than the self-determination, the flow and the goal setting theories, the self-efficacy is yet related to several other theories, including some outside of its category, namely "motivation and

affect". Its links with the ARCS model, the constructivist learning theory or the theory of planned behavior makes it a resilient framework. The notion of self-efficacy refers to "a person's subjective conviction that he or she can successfully perform the desired behavior". In other words, individuals with high self-efficacy are more likely to engage in challenging tasks, persist in the face of difficulties, and achieve higher levels of performance. Hence, this theory seeks to influence the factors related to the perception of "efficacy'. Bandura highlighted four main factors: "mastery experience, vicarious experience, social persuasion, somatic and emotional state" (Bandura,1994). The first one "mastery experiences", can be understood as the act of successfully performing a task. It's the most influential source of self-efficacy as it provides direct evidence of one's capabilities. Secondly, "vicarious experiences" refers to the act of observing others succeed. It can also enhance self-efficacy, particularly when the observer can relate with the model. Thirdly, the "social persuasion" is about encouragement from others. This factor can strengthen an individual's belief in their abilities. Finally, the last factor considers managing physiological and emotional states (such as reducing stress and anxiety) as a way to improve self-efficacy by influencing how one perceives their capabilities (Bandura, 1994, 1997).

These mechanisms collectively contribute to the development and enhancement of self-efficacy, which in turn influences motivation, behavior, and performance across various domains.

- **Learning: the constructivist learning theory**

Framed around the idea that social interactions play a crucial role in successful learning processes, Constructivist Learning Theory is one of the most popular theories used in the articles of the meta-review. From the "learning" category, other key theories can be mentioned such as the "cognitive load" theory, "experiential learning" theory, and "situated learning" theory. However, only the constructivist theory shares significant links with other categories, namely Self-Efficacy Theory and the Theory of Planned Behavior. Constructivism seeks to understand how people learn, and argues that individuals create new understandings using what they already know (Bada, 2015). Hence, learning is perceived as an active process, not a passive transmission of information. As Bereiter (1994) stated, "people construct their own understanding and knowledge of the world, through experiencing things and reflecting on those experiences."

Two key concepts within constructivism are accommodation and assimilation. On the one hand, accommodation refers to the ability of the participants to adapt and adjust to new realities after new experiences. On the other hand, assimilation can be understood as the process of integrating new experiences into the old ones. By having new experiences, the critical thinking of the participants is enhanced, as is their perception. Hence, this theory not only focuses on the construction and process of knowledge but also emphasizes the importance of motivation and goals in learning.

Additionally, the constructivist learning theory highlights four complementary elements that should be implemented to enhance the learning process. Firstly, "active learning" refers to the involvement of

learners who engage directly with the material through hands-on activities, problem-solving, and critical thinking (Jonassen et al. 1999). Secondly “experiential learning” complements the first principle by stressing the importance of learning through direct experiences and real-world applications, making the learning process meaningful and relevant (Kolb, 1984). Thirdly, “social interaction” allows learners to collaborate with peers, share perspectives, and construct knowledge collectively (Vygotsky, 1978). Moreover, “reflection” further enhances this process by enabling learners to evaluate their understanding and make necessary adjustments for deeper learning.

Therefore, the constructivist approach suggests that learners are motivated to understand their experiences and set goals to guide their learning processes. These aspects connect constructivism to Self-Efficacy Theory, which deals with an individual's belief in their ability to succeed, and the Theory of Planned Behavior, which explains how attitudes, norms, and perceived control influence intentions and behaviors (Bada, 2015).

- **Behavior: The theory of planned behavior (TPB)**

Initially theorized by Ajzen (1991), the Theory of Planned Behavior (TPB) is an extension of the Theory of Reasoned Action by adding the concept of perceived behavioral control. Its supporters argue that what makes people have specific behavior can be predicted by their intention to behave that way. These intentions are influenced by “personal attitudes”, “subjective norms” and “perceived behavioral control”. Firstly, “personal attitudes” (1) refers to the degree to which a person has a favorable or unfavorable evaluation of the behavior in question. This involves beliefs about the outcomes of the behavior and the value placed on these outcomes. For instance, if an individual believes that exercising will improve its health and values this outcome highly, he will have a positive attitude toward exercising. Secondly, the “subjective norms” (2) can be understood as the perceived social pressures to perform or not perform a behavior. These norms are based on beliefs about whether important people in the individual's life approve or disapprove of the behavior. If an individual perceives that their family and friends think they should exercise regularly, this perceived social pressure will influence their intention to exercise. Finally, the “perceived behavioral control” (3) refers to the individual's perception of the ease or difficulty of behaving. This perception is influenced by past experiences and anticipated obstacles. If an individual believes they have the necessary time, resources, and ability to exercise, they will have a higher perceived behavioral control, which strengthens their intention to engage in the behavior. (Hammady & Arnab, 2022; Brookes, 2023; Ajzen, 2020).

The interaction of these three factors determines the strength of an individual's intention to perform a behavior. A stronger intention increases the likelihood of the behavior being performed. This theory provides a framework for understanding how attitudes, social influences, and perceived control contribute to the formation of behavioral intentions and subsequent actions.

- **Mixed-categories: the ARCS model**

According to Krath et al., the ARCS model does not belong to any of the three categories, as the social cognitive theory. Nevertheless, it shares links with other theories such as the self-determination theory, self-efficacy theory and the reinforcement theory.

Developed by Keller in 1987, the ARCS model seeks to explain motivation through four components: "Attention, Relevance, Confidence, and Satisfaction". The first category, "attention" refers to the means used to capture participants' interest through "arousal" or "curiosity" to prevent boredom. These means can include challenges, surprises, exercises, or anything that can "stimulate perceptions" or "engage inquiry" as long as it's varied. Secondly, "relevance" ensures that educational purposes are aligned with learners' goals, their learning styles, and experiences, making the experience personally meaningful. In the case of cybersecurity awareness, this can be achieved by highlighting objectives and explaining their importance, especially in their daily life. Participants should be aware of the stakes for the company as well as their private lives. Increasing relevance can involve connecting goals to familiar environments for instance. In addition, "confidence" focuses on building participants' belief in their ability to succeed by setting clear expectations, providing opportunities for success, and "encouraging self-attribution" for success. For instance, integrating success opportunities with challenges or providing encouragement can enhance confidence. Finally, "satisfaction" aims to build a "sense of reward and achievement." It can generally be applied in three ways: firstly, through "intrinsic and natural consequences" by simulating real-world scenarios and their outcomes; secondly, by providing "extrinsic and positive consequences" such as immediate feedback; and thirdly, by ensuring equity in "learning and assessment." (Keller, 2016)

- **Mixed-category: The Social Cognitive Theory**

Related to the Self-Efficacy theory, the Social Cognitive Theory (SCT), was developed by Albert Bandura and seeks to understand how individuals learn and change behaviors through social interactions and observations. According to him, "humans are motivated to engage in different activities due to cognitive processes that use information resulting either from personal action or from the observed actions of others" (Ponton & Rheo, 2013). These processes are influenced by 5 features of the human's way of functioning. Firstly, "symbolization" refers to our ability to form "mental representations" of sensory experiences or information stored in memory. These mental symbols allow individuals to process and understand complex concepts and experiences even when they are not directly present. Secondly, "forethought" is the capacity to use these mental representations to envision future scenarios, which provides motivation and direction. Thirdly, "vicarious learning" is the process of learning by observing others, which allows individuals to benefit from others' experiences without needing to experience things firsthand, thereby avoiding potential risks. Fourthly, "self-regulation" is the ability to manage and direct one's own actions and behaviors to achieve

specific goals. Finally, the fifth characteristic is “self-reflection”. It involves thinking about and evaluating past experiences, which in turn influences future beliefs, attitudes, intentions, and behaviors. This last feature helps individuals learn from their successes and failures. These elements highlight the role of cognitive processes in SCT's understanding of human action (Bandura, 1978).

To summarize, several theories were developed in this review. Whether they focus on the motivation, the learning or the behavior, they all have the same object of study: people. Within the scope of the research, the objective is to find a strong theoretical framework in order to evaluate the efficacy of tested gamified solutions in order to find an alternative to traditional means of cybersecurity awareness. Hence, the selected framework must offer a multi-faceted lens, considering the capacity to enhance motivation, learning and behavior of the participants. People need to be motivated to willingly learn cybersecurity’s good practices and adapt their behavior as expected. As the objective is threefold, the theory should be connected to the three categories. Hence, the constructivist learning theory was selected. Its complementarity with self-efficacy and planned behavior theories makes it a relevant framework to evaluate motivation, learning, and behavior, as will be discussed in the next section.

3. Evaluating the efficacy of gamified solution: the constructivist learning theory

As more than a hundred theories could be considered as a framework to analyze gamified solutions, only a few, some of the main ones, were reviewed in the previous part. None of the theories has an approach which completely shares the three aspects, namely motivation, learning and behavior. Hence it was decided to select the constructivist learning theory. Its complementarity with self-efficacy and planned behavior theories makes it a relevant framework to evaluate motivation, learning, and behavior. As it shares link with these two other theories it provides a strong framework to evaluate the efficacy of the selected gamified solutions. Thus, this part will explore more in detail how the constructivist learning theory can evaluate the three criteria.

As argued earlier, the Constructivist Learning Theory defends that learners actively construct their own understanding and knowledge of the world through experiences and reflection on these. Several key principles can be highlighted. Firstly, “active learning” refers to the involvement of learners who engage directly with the material through hands-on activities, problem-solving, and critical thinking (Jonassen, 1999). Secondly “experiential learning” complements the first principle by stressing the importance of learning through direct experiences and real-world applications, making the learning process meaningful and relevant (Kolb, 1984). Thirdly, “social interaction” allows learners to collaborate with peers, share perspectives, and construct knowledge collectively (Vygotsky, 1978). Hence this theory is particularly well-suited for evaluating gamified solutions for cybersecurity

awareness as these solutions inherently involve active participation, interactive tasks, and problem-solving activities. Therefore, it aligns perfectly with constructivist principles. Consequently, the constructivist learning theory was used throughout the research, particularly in the methodology and the findings sections.

Conclusion & Summary

To conclude, this section's goal was to set the theoretical foundation of this research. After addressing the relevance and the context within which the thesis is anchored, a literature review of the theories was presented. A meta-review on the "theoretical foundation of gamification" brought key insights, underlining the theoretical landscape related to it. Hundreds of theories were used in various articles. Hence, only a few were presented for practical reasons. The "Constructivist Learning Theory" was selected as the main framework for this research because of its influence and links with other theories in the motivation and behavior categories. Moreover, the constructivist approach offers a rich analysis grid to analyze gamified solutions and assess their effectiveness.

Methodology: a quantitative approach

Introduction

This section presents the research design and methods used to explore the effectiveness of gamified solutions in enhancing cybersecurity awareness. The methodology is divided into 6 parts: the research question and hypotheses, the design framework, data collection and analysis techniques, and considerations for validity, reliability, and ethics. The primary goal is to provide a comprehensive overview of how the research was conducted and to ensure the reliability of the findings.

1. Research question and hypotheses

The aim of this work is to answer the following research question: **Which type of gamified solution is the most effective to raise cyber awareness?** Ensuring cybersecurity awareness acts as implementing a "human firewall". Hence, it matters to know how to effectively spread awareness about good practices in cybersecurity. As traditional methods are limited, gamification and serious games appear to represent a solid alternative. Nevertheless, as these concepts can be applied differently, it matters to assess which type of gamified solution could be the most effective. This assessment is relying on the results of the study but the criteria to evaluate the effectiveness comes from the selected theoretical framework. Hence, the aim of this work is to answer the following research question: "***Which type of gamified solution is the most effective to raise cyber awareness?***" Based on the theoretical framework and the constructivist learning theory, the following hypotheses were stated:

Hypothesis 1*: Gamified awareness sessions are more effective than traditional sessions in improving cybersecurity knowledge and behaviors.*

Hypothesis 2*: Gamified solutions that include high motivational elements (e.g., rewards, challenges) are the most effective in engaging participants and improving learning outcomes.*

Hypothesis 3*: Gamified solutions that incorporate diverse ways of learning (e.g., interactive tasks, simulations, multimedia) are the most effective in enhancing participants' understanding and retention of cybersecurity concepts.*

Hypothesis 4*: Gamified solutions that combine high motivational elements with diverse ways of learning are the most effective in improving cybersecurity knowledge, engagement, and behavior.*

These hypotheses are derived from the constructivist learning theory's principles and will be explored in the findings section. Each represents expected results based on the theory's principles. This section will further explain the research design and method used to validate or refute the above inferences.

2. Research Design

The structure of this subsection was influenced by John W. Creswell's book about "Research Design". According to him, the research design is composed of three main components: the philosophical worldviews (1), the selected strategies of inquiry (2) and the research methods (3). The first one refers to "paradigms" and can be defined as "basic set of beliefs that guide actions". The second one is related to "approaches to inquiry" and "research methodologies". Finally, the research methods can be understood as the method used to lead the research. (Creswell, 2014)

a. Philosophical Worldviews: under the prism of postpositivism

The philosophical perspective developed in this thesis is post-positivism. Also called "empirical science", this perspective recognizes that while objective reality exists, our understanding of it is inherently imperfect and subject to revision. This philosophy adopts a deterministic philosophy, arguing that "causes probably determine effects or outcomes" (Creswell, 2014). Consequently, this approach focuses on identifying and evaluating the causes influencing these outcomes, often through experiments. Its supporters argue that "there are laws or theories that govern the world, and these need to be tested or verified and refined so that we can understand the world" (Creswell, 2014). Following the scientific method, post-positivists begin with a theory, collect data that either supports or refutes the theory, and then make necessary revisions before conducting additional tests.

Although sometimes characterized as "reductionistic", this perspective seeks "to reduce the ideas into a small, discrete set of ideas to test, such as the variables that comprise hypotheses and research questions" (Creswell, 2014). Consequently, post-positivism appeared to be the appropriate philosophical perspective to lead this study.

b. Selected strategy of inquiry: use of a quasi-experimental design

This study adopted a quantitative approach using a quasi-experimental design and the survey method to provide a comprehensive understanding of the research question: "Which type of gamified solution is the most effective to raise cyber awareness?" The fundamental reason for choosing a quantitative approach is that it allows for a precise measurement of variables and statistical analysis of data to identify patterns, relationships, and differences among the various gamified solutions tested. By employing structured surveys, which included Likert-scale questions, the study quantified participants' levels of cybersecurity knowledge, motivation, satisfaction, and behavioral intentions before and after the interventions. This approach aimed to determine the significance of observed

changes and the relative effectiveness of each gamified solution. Consequently, the quantitative approach provided a robust framework for making data-driven conclusions about the impact of gamified interventions on cybersecurity awareness.

The quasi-experimental design was selected because it enables the estimation of "causal relationships without random assignment" (Creswell, 2014), unlike true experimental designs. Comparison groups were established and maintained for each test, and pre- and post-test measurements were collected through surveys. This design enabled the study to provide insights about the effectiveness of the gamified solutions in a controlled yet practical setting, reflecting real-world conditions where random assignment is often not feasible. Nevertheless, this research has several limits which will be explored later.

c. Research Method for data collection: pre- and post- surveys

As mentioned earlier, the survey was selected as the method of data collection. The questionnaires were available online for participants to complete. During the research project, five questionnaires were sent: three at the end of each test session[11], one before the start of the research project, and one at the end to conclude it.

The survey option was preferable for several reasons. Firstly, surveys provide a consistent framework for collecting data from all participants, ensuring that each individual is asked the same questions in the same manner. This standardization minimizes variation and enhances the reliability and comparability of the data collected. Secondly, as the aim was also to have precise measurement of variables such as knowledge, motivation, and satisfaction, "likert-scale" were often used in the forms. This quantitative approach enables the application of statistical tests to determine the significance and effect size of the gamified interventions. Thirdly, this method is time-efficient and cost-effective, especially regarding the data collection procedure. It can be easily created, adapted and then sent to the participants with only one link. Moreover, data collected through surveys can be easily managed and imported into Excel for analysis, reducing the potential for data entry errors and facilitating efficient data processing. Finally, the survey method was also chosen for its anonymous feature which encourages participants to have honest answers. It sets a benevolent and non-judgmental environment to have sincere answers about their cybersecurity habits, practices and opinions. Thus, by employing surveys, this study effectively captures the necessary quantitative data to evaluate the effectiveness of different gamified solutions in raising cybersecurity awareness, while also ensuring a robust and efficient data collection process.

[11] Only one survey was sent after the participants had tested the three selected e-learning.

3. Data collection & Data analysis

For the realization of this experiment, three main types of solutions were selected: one board game, three different types of e-learning and one escape game. Only the three e-learning were tested individually by the participants on their computers. These games were chosen after a study of the market and the offer in France. Hence, these games were selected for the variety of experience they offer but also their quality. The final decision resulted from a discussion (enhanced with several research on the topic) between the writer of this research and her supervisor during her internship over several other options.

a. Data collection: selection of games & population

Selection of the testes gamified solutions: description and justification

Three types of solutions were selected: one board game, two gamified (one partially, one extremely) e-learning, one escape game. They were chosen for several reasons that will be explained below, in addition to a detailed description of the tools.

- **Game A: Cybersecurity board game**

Game A is a board game based on a risk-based approach. Its objective is to raise participants' awareness of the importance of security measures needed to address risks, as well as to make participants active contributors to the security and compliance of their organization. Each participant or team represents an organization that must achieve sufficient compliance to reach the finish line. To improve compliance, players must prioritize risks and deal with event cards that can impact their organization. There are several sets of cards, including those on GDPR, ISO 27001 standards, and the fundamentals of cybersecurity. It is this last set of cards that was used for the test.

This solution was selected after comparing several different offers on the French market for "serious" board games dealing with cybersecurity. As only a few solutions exist, the chosen game was the one that seemed the more appealing and who was the most recommended. Moreover, contrary to other alternatives, this one had the possibility to be played with small or big groups.

- **Game B: E-Learnings**

Game B refers to three e-learnings tested by the participants. The first one is partially gamified while the second is much more. Finally, the last one is not gamified as “traditional” awareness e-learning. Game B.1 and B.2 were selected after reviewing the offer on the French market (through online research, recommendations, and during the International Cybersecurity Forum in Lille). These two solutions provide innovative alternatives that differ from traditional e-learning programs. Additionally, as they are fundamentally different, the user experience is also distinct but complementary for the purpose of this research. Lastly, Game B.3 refers to the more traditional

e-learning solution which was already in place within the company. All employees are familiar with it. The inclusion of Game B.3 provides a point of comparison for the participants, facilitating their responses to the questionnaires (the choice of the questionnaire will be further discussed later in this section).

- **Game B.1: Cybersecurity strongly gamified e-learning**

One of the three selected e-learning is strongly gamified, both in its aesthetics and the activities offered. Participants can engage in short “lesson” sessions within a gamified and interactive environment. In addition to these sessions, they can also participate in a "cyber cup." which includes a cash prize for the winner. This “cup” is a competition within a team or organization. To participate, users must earn tickets by completing lessons. With these tickets, they can access challenges that allow them to earn points and move up the leaderboard. Finally, this solution also includes summary sheets so the users can quickly reactivate the knowledge from previous lessons.

- **Game B.2: Cybersecurity partially gamified e-learning**

The second selected e-learning is partially gamified. It features an AI in the form of a chatbot that contacts participants directly via Teams, Slack, or email. The AI sends a message, inviting them to spend 5 minutes on a sensitization topic. The sensitization session takes the form of a brief exchange between the AI and the participant. The participant can choose from several responses during the course. Throughout the conversation, the AI adopts a relaxed tone and occasionally uses GIFs to make the interaction more enjoyable.

- **Game B.3: Cybersecurity non e-learning**

The last selected e-learning module is considered more "traditional" and serves as a reference point for the participants in the study. The e-learning is structured into several modules on different topics. Each module consists of text and audio content and includes a quiz at the end of each module.

- **Game C: Cyber Escape Game**

Finally, the last selected game is a "Cyber Escape Game." Similar to a traditional escape game, participants are invited to immerse themselves in a scenario and solve various puzzles to reach the final objective. In this study, players took on the roles of spies searching for confidential documents. The story takes place in the (fictitious) office of the CFO. Because the CFO employs several poor practices, participants have the opportunity to infiltrate and find this information. The themes addressed in this escape game included passwords, social engineering, access management, GDPR, and more. As a bonus, at the end of the session, an interactive and gamified quiz was provided via a gamified platform. An escape game offers an immersive experience where employees must

collaborate to achieve various objectives. Players are immersed in a relatable situation: their everyday office environment. Consequently, participants have to navigate through both good and bad practices within the scenario to reach their setted goals. Thus, this third type of game was selected, in part, for the immersion it promises.

Selection of the sample: the population

The population was selected on a voluntary basis. As it took place in a consulting company (internship), most of the participants had busy schedules which limited the number of participants and tests. Thus, only 19 people were selected. They are all working for the same organization but have different work and teams. Participants were selected on the basis of their field of work and education, in order to have a diverse sample. Hence, two profiles can be highlighted among the participants. On the one hand, some were more "experts" (SOC/CERT, Pentseters, consultants…) in cybersecurity, while on the other others could be considered as "non or less experts" (finance, HR, recruitment). Other characteristics such as gender, age or origins were not taken into account through the selection process though parity was tried to be achieved.

b. Data analysis: descriptive statistics and assessing effectiveness

Surveys: Analysis of the results

As the data was collected through Microsoft Forms (through surveys), it was easily managed and imported into Excel for the analysis. The interoperability of these tools reduced the risk for data entry errors and facilitated the data processing. Therefore, to analyze the results of the surveys, the method of descriptive statistics was used. In other words, the data was summarized using measures of central tendency (mean, median) and measures of dispersion (standard deviation) to provide a clear overview of the participants' responses. Additionally, graphical representations such as bar charts were used to visually illustrate the distribution of responses. This approach enabled a comprehensive understanding of the general trends and patterns within the data, setting the stage to evaluate the effectiveness of the different gamified solutions in raising cybersecurity awareness.

Using the results to assess the level of effectiveness

To assess and compare the level of effectiveness of each tested solution, the concept of "effectiveness" must be approached. As argued in the previous section, a gamified solution can be evaluated by taking into consideration three criterias: motivation, learning and behavior. Therefore, the proposed method of assessment relies on it and the constructivist learning theory. According to the constructivist approach, effective learning environments are characterized by active learning, experiential learning, social interaction, and reflection. These principles guide the assessment of the gamified solutions in terms of their ability to engage participants, facilitate knowledge acquisition, and promote behavioral

change. By understanding these foundational elements, we can better structure our evaluation to measure the effectiveness of each gamified solution.

Firstly, to evaluate motivation, the engagement and enjoyment experienced by participants during the gamified sessions are considered. Active engagement, a key aspect of the Constructivist Learning Theory, involves learners interacting directly with the material through hands-on activities and problem-solving (Jonassen, 1999). This conceptual aspect will be taken into consideration for each gamified solution. Moreover, questions in the surveys are designed to evaluate the perceived enjoyment or boredom felt by the participants.

Secondly, to evaluate learning, the extent to which each gamified solution approaches knowledge acquisition and reinforcement is discussed. Experiential learning, as emphasized by Constructivist Learning Theory, stresses the importance of learning through direct experiences and real-world applications (Kolb, 1984). Similar to the evaluation of motivation, specific questions are added to the surveys to measure perceived knowledge gains. Additionally, the functionalities and components of each game are analyzed to provide an initial understanding of the educational value of each solution, although the limitations of the study preclude more detailed results.

Lastly, to evaluate behavior, the impact of the gamified solutions on participants' cybersecurity practices and confidence in their abilities is considered. Behavior change, an essential outcome of effective cybersecurity training, reflects the practical application of learned knowledge. “Social interaction”, another core principle of Constructivist Learning Theory, facilitates collaborative learning and peer influence on behavior (Vygotsky, 1978). This is assessed through survey questions on behavior changes and confidence levels. These assessments provide insights into the extent to which the gamified solutions motivate participants to adopt and maintain secure cybersecurity behaviors and enhance their confidence in handling cybersecurity threats.

By defining and measuring effectiveness through the lenses of motivation, learning, and behavior, under the umbrella of the Constructivist Learning Theory, this research aims to identify the most effective gamified solution for enhancing cybersecurity awareness. This comprehensive approach ensures that the selected solution not only engages participants but also fosters deep learning and promotes lasting behavioral change.

To conclude, the data analysis relies on two features. On the one hand, the pre- and post-session surveys which bring the quantitative aspect of this research. On the other hand, the questions and the surveys were shaped and influenced by the constructivist approach as developed above and in the theoretical framework. Finally, the results of this analysis will be presented in the Finding section.

4. Validity & Reliability

Validity and reliability are two concepts at the core of any research design. Both assess and indicate the consistency and accuracy of a study. Despite some limitations (time, logistics, context, etc…), validity and reliability were addressed throughout the research process. Firstly, internal validity was maintained through the process by keeping the same groups through the experience which allowed them to compare the different gamified solutions. Moreover, a pre-test survey was sent to the participants to measure their opinion on gamification and serious games but also to assess their cybersecurity expertise, and level of confidence. Secondly, external validity was addressed by selecting "expert" and "non-expert" profiles. As they were all from a cybersecurity company, having a more diverse population was not possible. Then, reliability was addressed by using a standardized survey format and maintaining consistent and similar conditions for all participants to minimize potential variability. Each group tested the 5 gamified solutions, and their responses were collected and analyzed to identify patterns and draw comparisons. Hence, reliability and validity were addressed as much as the context of the study allowed. Despite limits it offers an insight for future perspective of research.

5. Ethical Considerations

Ensuring ethical consideration was considered since the beginning of the research. In this respect, several measures were included in the ethical and acceptance form sent to the participant before the beginning of the research. Annexe n°1 presents the original version in French in addition to its translation in English of this agreement.

Firstly, participants were informed before participating in the study about its purpose, the procedures and their role. Indeed the study had a double aim, on the one hand answering to the topic of my internship (*The market and stakes of the gamification of cybersecurity*), on the other hand, the research question of this master's thesis (*Which type of gamified solution is the most effective to raise cyber awareness?*). Therefore, the purpose of the study was summarized with the following question: "Are games an effective solution to enhance cybersecurity awareness?". Secondly, participants were informed about confidentiality and anonymity. All the data collected were anonymized with an ID tag (for instance ID_1 for participant A). Nevertheless, participants also had the opportunity to register with nicknames in order to keep their identity confidential. Thirdly, participants were informed about their right to withdraw from the study and without any negative consequences. Moreover, the study was designed to minimize any potential risks or stressful situations. Finally, the collected data is solely used for the purposes stated in the agreement, (master's thesis and internship). After being used, processed and analyzed, the data was deleted. Before being deleted, the data was stored in a secure area accessible only to a few authorized people.

Hence, these measures set up the basis to build an ethically led study in order to ensure participants' rights and well-being throughout the research process.

6. Limitations

This methodology has several limitations that must be highlighted. Firstly, the particularities of the population and its selection limit the generalizability of this research due to potential errors and biases. The selected sample is relatively small, only 19 participants. Additionally, despite being from different departments, all participants knew each other as they were from the same organization. The voluntary nature of participation might result in self-selection bias, where participants with a higher level of interest or prior knowledge in cybersecurity, or a stronger inclination towards games, choose to participate. This bias could lead to an overestimation of the effectiveness of gamified solutions, as these participants may already be more inclined to engage with and benefit from such interventions. Therefore, these characteristics could introduce errors or biases. Future research could address this limitation by using a larger and more diverse sample, along with a more randomized recruitment process to ensure a representative sample.

Secondly, as the study relied on self-reported data collected through surveys, other potential biases must be taken into consideration. One could be the social desirability bias, where participants might provide responses they believe are expected or favorable rather than their true opinions or behaviors. This can lead to inaccuracies in the data collected. Furthermore, self-reported data can sometimes be unreliable due to participants' misinterpretation of questions or varying perceptions of the response scales. To mitigate these limitations, future research could incorporate a mixed-methods approach, combining quantitative surveys with qualitative methods such as interviews or focus groups. This approach would provide a more comprehensive understanding of the effectiveness of gamified interventions in cybersecurity awareness. Additionally, as some participants already had at least prior if not strong knowledge in cybersecurity, the answers regarding the "learning" are biased. A cybersecurity expert won't learn new things during a cybersecurity awareness session which initially targets a beginner population. Moreover, this study lacks a tested solution for comparison. If indeed, three e-learning games were tested, only one board game and one escape game were tested. Consequently, participants' answers lack elements of comparison. Hence, as it will be developed in the findings, the results of the board games are rather high compared to the other games, though it is only ranked at the third position. This can be explained by the fact that this game was the first to be tested.

Finally, as this research served two different purposes—one for a master's thesis and one for an internship—the selection of participants and tested solutions were influenced by considerations related to both objectives. The dual aims implied a balance between academic "rigor" and practical

applicability within the organizational setting. This dual purpose may have introduced certain constraints, such as the limited availability of participants and the selection of gamified solutions that were feasible and relevant within the internship context. While this approach ensured that the study addressed real-world challenges and provided valuable insights for the organization (internship), it also restricted the range of solutions tested and the diversity of the participant sample.

These limitations highlight the need for future research to explore a broader array of gamified interventions across varied settings to enhance the generalizability and applicability of the findings.

Conclusion & Summary

To conclude, this section presented the methodology foundation of this master's thesis. This study adopted a post-positivist philosophical perspective, aligning with a quasi-experimental design to quantitatively assess the effectiveness of gamified solutions in raising cybersecurity awareness. Additionally, data collection involved pre- and post-surveys, enabling measurement of variables such as knowledge, motivation, and satisfaction. Three types of gamified solutions—board games, e-learnings, and an escape game—were selected for their diversity, originality and quality in order to ensure a comprehensive evaluation. To analyze the results, descriptive statistics were used. It provided clear insights into participants' responses and facilitated the assessment of each solution's effectiveness. Validity and reliability were addressed through consistent survey formats and controlled testing conditions, while ethical considerations ensure participants confidentiality and the right to withdraw. Finally, regarding the limits, they significantly impact the generalizability and reliability of the findings. The small and homogenous sample size, combined with the voluntary nature of participation, introduces selection bias that could skew the results. The reliance on self-reported data further compounds these issues, as it is susceptible to social desirability bias and inaccuracies. Additionally, the participants' prior knowledge in cybersecurity and the limited range of gamified solutions tested constrain the breadth and depth of the conclusions. The dual purpose of the study also imposed practical constraints, affecting the selection of participants and tested solutions. Future research should address these limitations by employing larger, more diverse samples, randomized recruitment, and mixed-methods approaches to enhance the robustness and applicability of the findings.

Literature Review: Games as the key to effective cybersecurity awareness?

Introduction

Integration of game elements into non-game contexts has recently attracted significant attention, leading to the development of two closely related concepts: gamification and serious games. The primary aim of this literature review is to explore how these concepts can be effectively utilized to enhance cybersecurity awareness and ultimately reduce human risk.

Therefore, this review examines the concept of cybersecurity awareness training, its different methods and effectiveness. It is structured in two main parts. The first one will explore the conceptual framework of cybersecurity awareness, and examine the "traditional" cybersecurity awareness methods. In a second time, this section will focus on the efficacy and constraints of gamification and serious games as innovative tools for enhancing cybersecurity awareness. By exploring both the promises and challenges of gamified solutions, this literature review seeks to provide a comprehensive understanding of their effectiveness and limitations.

1. Traditional awareness methods and its limits

Conceptualization: Cybersecurity awareness or training ?

Cybersecurity awareness or training are central programs to enhance security among organizations (private or public). This allows information to be spread to all members of the group, regardless of their role or position, and according to their needs (Alruwaili, 2019). Nevertheless, "awareness" and "training" are not completely the same things. This distinction matters as both concepts focus on different sides and degrees of cybersecurity "knowledge". The NIST Special Publication (NIST SP 800-50[12]) defined "cybersecurity awareness" in opposition to "cybersecurity training" by arguing that "awareness is not training". The purpose of the awareness presentation is to "allow individuals to recognize IT security concerns and respond accordingly". Hence, cybersecurity *awareness* involves understanding the importance of cybersecurity and recognising potential threats. Cybersecurity *training* focuses on teaching specific skills and behaviors to mitigate these threats in order to perform a job more securely. (NIST SP 800-50). Despite these differences, both training and awareness are complementary. Bada et al. (2014) highlighted that awareness by itself was not enough, it should be "complemented by effective training". The fusion of both methods enhance individuals' understanding of risks and how to effectively respond.

[12] NIST SP 800-50: *Building an Information Technology Security Awareness and Training Program (Published in 2003)*

Nevertheless, this research will primarily focus on cybersecurity awareness. To explore in more detail its definition(s), it is possible to highlight several points that are commonly found across various conceptualizations of cybersecurity awareness. Generally, it can be defined as “thoughtfulness on security, enabling individuals (workforce employees and managers) to recognize security concerns and respond accordingly” (Rieff, 2018). Other scholars such as Al-Daeef et al (2017), understand it as a “continual process of learning” enabling the participant to “realize the importance of information security issues”. Additionally, it is also possible to set a wider definition of cybersecurity awareness by defining it as “the ability of the user to recognize or avoid behaviors that would compromise cyber security; practice of good behaviors that will increase cyber security; and act wisely and cautiously, where judgment is needed, to increase cyber security” (Toth & Klein, 2014). To summarize, the aim of cybersecurity awareness is to pass on knowledge and good practice to people who have little or no prior knowledge of the subject - in our case, cybersecurity. Nevertheless, it can also be used to remind people who are already aware of good practice.

Traditional cybersecurity awareness and its limits

Traditional cybersecurity awareness training typically employs means such as (live or recorded) conferences, written documents, or (online) sessions similar to lectures. These methods are straight to the point and seek only to answer the objectives setted in the cybersecurity awareness strategy. Most of the time, the aim is to inform employees about cybersecurity risks and encourage them to adopt good practices. However, several studies have highlighted significant limitations associated with these approaches. The issue is not in the knowledge that is shared but in how it is done.

Firstly, traditional methods are often characterized as “unable to engage participants” effectively, leading to poor retention and application of knowledge. In her article, Rieff (2018) argued that these methods such as “e-learning” or “regular presentations” are usually perceived as “intimidating, time-consuming, and non-inviting." This lack of engagement results in employees not internalizing the critical information they need to improve their cybersecurity practices. Moreover, according to Bada et al. (2015), traditional training methods fail to "adequately address the dynamic and evolving nature of cybersecurity threats." Thus, as cyber threats continuously change, traditional methods quickly become outdated and less effective. This gap between evolving threats and traditional awareness limits the practical impact of cybersecurity awareness. Similarly, Aloul (2012) pointed out that these methods are perceived as impersonal and too generic. Consequently, they diminish their impact on actual user behavior. The scholar argued that "traditionally, information security has been viewed as a sort of service that has to be provided, instead of something that influences people." This perspective results in training programs that do not “resonate” with employees on a personal level, reducing their effectiveness. Finally, Al-Daeef et al. (2017) discussed the broader implications of traditional training's shortcomings. They note that while there have been claims that information

security awareness does not work, well-designed user training methods can effectively enhance awareness and adoption of security behavior. Although awareness-raising is effective, both traditional and gamified, it is still perceived as secondary by both companies and employees. Consequently, users feel they do not need to be trained and to adopt the good practices. Additionally, as their study suggested, "technology-related mistakes" made by users cannot be resolved by simply adding more technology. Instead, awareness-based training programs are needed to mitigate the limitations of technology-focused security solutions.

To sum up, while traditional cybersecurity awareness training methods have been the "standard approach" for the last decades, their limitations in engagement, relevance, motivation and personalization, etc, call for a reevaluation of how organizations spread cybersecurity awareness to their employees. Moving towards more dynamic, interactive, and personalized training programs such as gamification or serious games could represent a relevant alternative.

2. Cybersecurity awareness & gamified solution

Promises of Gamification & Serious games: what are the differences with traditional methods?

Gamified solutions have emerged as innovative approaches to enhance cybersecurity awareness. Considered as an effective alternative to the traditional approaches, these methods are supposed to influence and enhance motivation, learning and behavior. This subsection will address the academic literature on the expected effectiveness from a broader perspective, extending beyond cybersecurity awareness while remaining within the scope of education. Several features of gamification and serious games were highlighted as enhancing the effectiveness of awareness.

On the one hand, scholars argued that games offer a more personalized learning experience with the possibility to access immediate feedback. Learners receive instant responses to their actions, allowing them to understand mistakes and correct their behavior in real-time. This feedback is crucial for reinforcing "correct behaviors" and consequently, enhancing the participants' confidence in their action and knowledge. On the other hand, another highlighted advantage of gamified cybersecurity awareness is the importance of collaboration and social interaction. Games often incorporate multiplayer elements and team-based challenges that require participants to work together to solve problems and complete tasks. This collaborative aspect promotes and encourages communication and teamwork, essential skills for maintaining robust cybersecurity practices in real-world settings. According to Buckley and Doyle (2016, p.19), social interaction in gamified environments can enhance learning by allowing users to share knowledge, strategies, and experiences, further solidifying their understanding of cybersecurity concepts. In the context of a company or an organization, it can also reinforce team building and teamwork among colleagues. As for the previous point, social interaction represents a source of inspiration and increases confidence. Additionally,

most scholars argued that games provide **a safe environment** for users to experiment with different cybersecurity strategies without the risk of real-world consequences. This aspect of gamification is particularly valuable in cybersecurity awareness, where making mistakes in real "life" could have severe consequences. In a gamified environment, users can test various approaches to handle cyber threats, learn from their errors, and enhance their techniques. Alruwaili (2019, p.16) emphasized that this safe experimentation environment is crucial for developing practical skills and building confidence in managing cybersecurity threats. Learners can explore different scenarios and tactics, receiving feedback that helps them understand the impact of their decisions and improve their problem-solving abilities.

These features influence the motivation, learning and behavior, three categories at the core of gamified solutions. Hence engagement and motivation were often mentioned as enhanced by gamified methods. As argued earlier, traditional cybersecurity training methods often fail to captivate participants, resulting in low retention rates and minimal behavioral change. Gamification, on the other hand, integrates game elements such as points, badges, and leaderboards, fostering a competitive and enjoyable environment. This gamified environment motivates users to actively participate in training programs. Furthermore, Hamari et al. (2014, p.20) argued that these game elements significantly improve user engagement and motivation, leading to more effective learning outcomes. Similarly, Alruwaili (2019, p. 15) found that gamified cybersecurity training led to higher levels of engagement and improved knowledge retention among participants. Additionally, retention and understanding are also increased. The interactive and practical applications within game-based learning environments help reinforce users' understanding and memory. Baral and Arachchilage (2019, p. 102) demonstrated that game-based learning significantly enhances users' ability to retain information by requiring them to apply learned concepts in simulated environments. This is particularly effective in scenarios where users need to identify and respond to cyber threats. For instance, "anti-phishing games", improve users' detection skills more effectively than traditional methods (Baral & Arachchilage, 2019, p. 105). Finally, the capacity of games to change participants' **behavior** was also highlighted in the articles. For instance, repeated exposure to realistic cyber threats in a controlled environment helps develop a security-first mindset, translating into safer online practices. Bada et al. (2015, p. 25) noted that gamification elements like competition and storytelling significantly enhance users' motivation to adopt secure behaviors.

Hence, most of the research and articles concluded that gamified solutions had a positive impact in awareness. For instance, in their article, Hamari et al. (2014) analyzed several empirical studies on gamification to evaluate whether or not "gamification works"? To answer this question, they evaluated the implemented "game-like motivational affordances" in addition to the elements used to influence the behavioral outcomes. After analysis they indeed found that gamification has positive outcomes. However, they found that such results depended on the context and the users. Similarly, in their meta-review, Krath et al. found that gamification is not "effective per se" but more that the

effectiveness depended on the quality of the design. Hence when the appropriate framework is used, results were indeed positive. Iris Rieff, in her article confirms this argument: gamified solutions are effective when properly designed and implemented.

In summary, studies have shown that games represent an alternative to the traditional methods to spread awareness as it influences behavior, the learning experience, and the motivations. Nevertheless, results are not guaranteed and some limits must be brought to the light.

The limits of a games for cybersecurity awareness

Despite its effectiveness, gamified solutions have limits that must be highlighted. Firstly, the effectiveness depends on the **quality design** (1) of the solution. As mentioned in a previous part, gamification and serious games are not "effective per se" (Krath et al. 2021). Poorly designed games can fail to engage users or convey the intended educational content effectively. Baral and Arachchilage (2019) argued that a poorly designed game could lead to the opposite effect. For instance, it could generate frustration, disengagement among users and thus, undermine the educational objectives. Hence the success of gamified training programs relies on careful planning and execution, ensuring that the game mechanics align with the educational goals.

Secondly, if the **balance between amusement and education** is not well managed, there is a risk that users may focus more on game mechanics than on learning the actual content (2). Bada et al (2015) highlighted that while gamification can enhance motivation, it can also lead to distractions if users are more interested in achieving game-related rewards than in understanding cybersecurity concepts. Likely, Rieff (2018) supported this view, adding that some participants in gamified simulation were more focused on winning the game rather than absorbing the cybersecurity lessons. Consequently, it can result in a superficial understanding of critical concepts, which could undermine the effectiveness of the training. In the same way, certain scholars observed that by using games, the solutions are lacking in "deep learning". Bada et al. (2015) observed that while gamified elements can make learning more enjoyable, they do not always ensure that users develop a profound understanding of cybersecurity principles. Rieff (2018) echoes this concern, emphasizing that the focus on game mechanics and rewards can sometimes overshadow the educational content, leading to a less thorough grasp of the material. Effective gamified training should balance engagement with substantive learning to ensure that users not only enjoy the experience but also gain meaningful insights into cybersecurity practices.

Thirdly, despite effective results, the research reveals **variable effects** (3). Hamari et al. (2014) found that while some users benefit greatly from gamified learning, others may not respond as positively. According to Rieff (2018) it can be explained by individual differences such as "prior experience with games", "learning preferences", and "personal motivation levels" which can significantly influence the outcomes of gamified training. This variability highlights the need for careful consideration of the target audience and customization of the training program to meet their specific needs. Not all game

elements may be universally engaging or educational for all participants.

Moreover, most of the studies are rather recent and present important limitations, precisely when it comes to the **long-term effect** (4) of gamified solution. Rieff (2018) and Alruwaili. (2019) observed that the novelty effect of gamification might wear off over time, reducing its long-term impact if not continuously updated and improved. While initial participation rates in gamified training are often high, sustaining this engagement over the long term can be challenging without continual updates and new content. Hence, gamified solutions should regularly refresh the content and game elements to maintain user interest.

Conclusion & Summary

Gamification and serious games are two increasingly popular concepts used across various domains, including health, marketing, and team building. In education, several studies have explored the use of these concepts. However, in the realm of cybersecurity awareness, research is less extensive and diverse. This literature review first examines traditional methods, such as conferences and online sessions, which often fail to engage participants and quickly become outdated. Secondly, the review highlights that gamification enhances engagement and retention, although its effectiveness relies on quality design and regular updates. Despite their potential, poorly designed games can cause frustration and superficial learning, emphasizing the need for careful planning and adaptation to sustain long-term interest.

Findings: which gamified solution is the most effective?

Introduction

As developed in the literature review, games indeed appear to be a relevant alternative to the traditional methods to spread cybersecurity awareness. Hence, the aim of this section is to provide an answer to the research question: Which type of gamified solution is the most effective to raise cyber awareness? To do so, this section will first look at the results of the case-by-case tests. Each solution tested will also be examined, taking into account the motivational, educational and behavioral aspects. The results will then be compared to provide an answer to the research question. The hypotheses will also be confirmed or refuted. To this end, the analyses in this section will be carried out under the prism of the selected theory: the constructivist learning theory.

1. Analysis of the results: case-by-case overview

Five, more or less gamified, solutions will be analyzed and reviewed in this section. After each test, participants had to fill a survey with several recurrent affirmations to which they had to answer “completely wrong, rather wrong, rather true or completely true”. The aim was to assess the motivational, educational and behavioral prospects. The results will be considered in addition to the constructive elements of the solutions.

A. Game 1: The board game

The first tested game was a board game. Based on a “risk approach”, the aim is to raise participants' awareness regarding the importance of the security measures needed to deal with the risks, and to make them responsible for the security and compliance of their organization. Each participant or team represents an organization that must achieve a sufficient level of compliance to cross the finishing line. To improve their security, players must prioritize risks and manage “special event cards” that could impact their organization.

Regarding the motivation it was found that most participants had fun or enjoyed the session, 27% rather true and 73% completely true and none was bored through the session. All appreciated the teamwork and it was not perceived as infantilising. Nevertheless, from the practical perspective, some reservations may be expressed regarding the motivational capacity of this solution. On the one hand, the game, which can be played in teams, encourages participants to give their best and participate actively in order to be the first to cross the finish line. But on the other hand, the competitive “spirit” is not a universal source of motivation and can generate stress or anxiety. Coupled to the randomness

dimension linked to the dice rolls and card draws, it can create disadvantages to some groups, reducing motivation and generating frustration. As a result, groups that make efforts to protect their organization are not always rewarded due to the game's random elements. Secondly, the educational results were also highly ranked with over 80% of the participants answering positively to the question “I strengthened my knowledge” and “I learned new things”. This can be explained by the original perspective of the game. This board sought to transfer knowledge through a risk-based approach which simulates an organization's protection facing “feared events”. This perspective, where participants put themselves in the shoes of an organization that needs to protect itself, is not a common one. Nevertheless some limits can also be highlighted. If participants can learn more about the risks by scanning QR code or by discussing the right measures to implement, the learners are often carried away from the game and strategy, neglecting the ultimate goal: learning. Therefore, the balance between enjoyment and learning is weak.

Thirdly, regarding the behavior, participants had mixed answers. Around 60% do not feel motivated to change their behavior after the session and 40% argue that they don’t feel more confident in their knowledge and capacities. One of the reasons could be the format of the game. The tested board game puts more emphasis on understanding security and how it works within an organization than on what each participant can do on a day-to-day basis. Though there are cards highlighting bad practices such as leaving your computer unlocked or having your password on a post-it note, the players remain detached from ‘reality’.

In conclusion, the game was appreciated, but its effectiveness is debatable. Regarding motivation, despite the positive aspect of teamwork, certain elements can lead to frustration and counterproductive effects. In terms of learning, fun and strategy can easily overshadow the primary goal: understanding the importance of securing one's organization. Consequently, participant's behavior remains largely unchanged. Although some cards highlight poor practices and security flaws, participants are not strongly encouraged to change their behavior. For example, if one of the bad practices is writing passwords on a post-it note, the solution would be to use a password manager. However, practical solutions are not emphasized. For more information, participants can scan a QR code, but none of them considered doing so, partly because it interrupts the flow of the game. Thus, the problem might lie more in the game's design than in its general format (board game). Additionally, it is possible that the game was not well-organized or integrated by the game master. It is conceivable that integrating it into a more structured awareness session with a game master encouraging participants to read their cards and reflect, along with the addition of a quiz at the end, could make this tool more effective.

Hence, despite good results, this game was ranked at the third place by the participants. This discrepancy in results and ranking can be explained by the fact that it was the first tested game which might have led participants to give overly positive answers as they had no elements of comparison.

B. Three shades of e-learnings

For this research, three models of e-learnings were selected on the basis of their approach to gamification. One is highly gamified in its design and user experience, while the second is partially gamified with only a chatbot sourced by AI. The last one is closer to a traditional e-learning plateform. The participants had the opportunity to test these solutions for 2 weeks and then had to fill the survey. Thus, this part of the research was conducted by participants on their own, as e-learnings are generally not a group activity.

- Game B1: The fully gamified e-learning

The “game B1” refers to a fully gamified e-learning platform. It is structured in several parts. Firstly, participants took parts to “micro-session” with highly gamified designs and mechanics. During this session, the learners had a first approach with the concepts. Then, in a second time, they had access notes summarizing the key points of the notions they learned. Finally, in a third time, participants could participate in a “Cyber Cup”, a competition held within a team or organization. With each attempt, the player used previously earned tickets after each micro-session. Based on their score, they ranked higher or lower on the leaderboard. At the end of this "Cyber Cup," players could win a cash prize.

Firstly, the questions related to the assessment of motivation, had positive results. None of the participants declared to have felt boredom. Around 67% of participants answered rather true and 33% completely true, to the affirmations related to enjoyment. Such high results for this e-learning can be explained by several features at the core of the solution. As every e-learning, it is normally conducted individually with the exception, here, of the “Cyber Cup” rush periods. Every three months, for two months, users can compete on the leaderboard to win a cash prize. These two elements enhance motivation and engagement, especially during competition periods. Nevertheless, it is possible that some participants did not feel motivated by the competition and might have dropped out early, assuming they will never win the prize for instance. This aspect also aligns with the individual nature of the solution.

Secondly, regarding learning, this solution offered the opportunity to learn from three different ways and means: micro-session, challenges, and notes. This difference of learning ways can stimulate the process of learning. Hence, the learning process is divided into three parts, to ensure that the concepts are firmly rooted, particularly through practice and repetition. Nevertheless, some elements of the solutions were characterized as redundant or even infantilising such as the repeated use of GIFs. Consequently, only 50% of the learners think they have learned new things, and around 60% believe they have strengthened their knowledge.

Thirdly, regarding the behavior, results are high. More than 90% of the answers indicate that the participants were motivated by this solution to change their behavior and that their confidence in their skills was enhanced and strengthened. This can be explained by the dynamic and stimulating environment built by the solution. By increasing the confidence of the participants, it strengthens their confidence in adopting the right behaviors.

To conclude, this solution was highly appreciated by the participants despite its limited use of 2 weeks. At times infantilizing or redundant in its functionality, it seems that its originality managed to make participants forget that it was an e-learning platform. Thus, this ultra-gamified model, reinforced by the "lure" of cash prizes, competition periods, and leaderboards, seems to strengthen participants' engagement over time. Ranked at the 2nd place out of 5, it appears to be a good alternative to the traditional e-learning format.

- **Game B2: The partially gamified e-learning**

The "game B2" can be described as partially gamified. It is built around a personified AI as a chatbot that contacts participants directly via Teams, Slack, or email. The AI sends a message inviting participants to spend approximately 5 minutes on an awareness topic. The session took the form of a brief exchange between the AI and the participant. The learners can choose from one or two responses during the session. Throughout the conversation, the AI adopts a relaxed tone and sometimes uses GIFs to make the interaction more enjoyable.

With respect to motivation, learners expressed a mixed opinion. On the one hand, most users did not find the solution really "fun" but on the other hand, they did not express boredom. Nevertheless, 58% felt infantilised by the AI through their sessions. This solution does indeed lack motivation elements. One of the only motivating aspects might be the AI's personality, which does not appeal to everyone. Additionally, the repeated use of GIFs and the limited choice of responses hinder the user experience. Finally, unlike the other tested solution, this one is only structured around the AI, for instance there are no leaderboards or interactions beyond those with the AI.

Regarding the learning strategy of this solution, 40% of the participants agree that they have learned new things while 58% have strengthened their knowledge. Despite individual learning sessions, the micro-sessions were clear, accessible, and it was possible to ask the AI questions outside of the sessions. However, the experience remained limited. This solution only includes one quiz per year and no memo sheets to reinforce the knowledge covered. Hence, the educational prospects of these solutions are lukewarm.

Thirdly, the participants all agreed feeling more confident after their micro-session with the AI and 67% felt motivated to change their behavior. During the micro-sessions, the AI suggested and invited learners to adopt new practices related to the discussed topics. The AI clearly pushed participants to

understand the benefits of adopting these changes. However, this does not significantly differ from a traditional e-learning experience.

To put in a nutshell, although this solution offers an original alternative to the traditional e-learning format, the user experience still resembles it. Moreover, it is ultimately quite limited compared to traditional e-learning because there are no memo sheets, summaries, or quizzes to challenge the learning. Its detachment from a platform was initially seen as an advantage to more easily reach employees, but it can prove to be counterproductive. Nevertheless, Game 2.B was ranked at the 4th position. Compared to other solutions, it could be considered the "most restricted" in its functionalities. Its integration with Teams is practical and interesting, but the value of interactions with the AI, the excessive use of GIFs, the limited response choices, etc., penalize the effectiveness and appreciation of it.

- **Game B3: The non-gamified e-learning**

The last tested e-learning has a more traditional structure. Composed of a few short sessions of 10 min maximum, it goes straight to the point. Each session firstly presented the notion, its challenges, and its importance. Then, the participants had to pass a quiz to validate the module. Each session focuses on a topic such as phishing, social engineering; GDPR, etc… This solution was developed by the company where I did my internship. Thus, all employees joining the company have to complete it. This is an important detail that may have influenced the answers.
As with most traditional methods and e-learning, we could've expected strong opposition to game 2C notably because of its lack of motivation elements. Nevertheless, the results were mixed. On the one hand, 67% did not found this solution enjoyable or "fun" while on the other hand, 58% declared that it was not boring. Hence, although not very "amusing" this solution is no less interesting according to the participants. This can be explained by the structure and the aesthetic of the platform which is not gamified but clear and easy to understand.
When it comes to the learning criteria, results are high as 75% of the participants felt that they had learned new things and 90% that they had reinforced their knowledge. This solution seeks to spread the messages as clearly and easily as possible. It's straightforward and confirms the elements of the session with a final quiz at the end.
Finally, regarding the change of behavior, results are similar to the ones for the learning category. Most participants felt that they are more confident in their capacities and skills and consequently, that they are more willing to change their behavior accordingly.

To sum up, this more traditional e-learning surprisingly has positive feedback from the participants though it was ranked at the last position, and ended at the fifth place. The fact that this solution was developed by the organization where the internship and experiment took place might have affected the

answer. It’s possible that the participants, though the answers were anonymous, did not want to give negative feedback to a solution internally produced.

C. Game 3: The “Cyber Escape Game”

The escape game with a cybersecurity approach was the last tested solution. Like a traditional Escape Game, the learners were invited to immerse themselves in a scenario and solve various puzzles to reach the final objective. In the developed scenario, participants played the role of spies searching for confidential documents. The story took place in the (fictitious) office of the CFO. The participants had to infiltrate the office and resolve challenges and enigmas based on good and bad practices. Players were plunged into a realistic situation: their daily work environment. The thematics addressed in this escape game included passwords, social engineering, access management, GDPR, etc. Additionally, at the end of the session, an interactive and gamified quiz was planned via a gamified platform.

Firstly, the escape game format is inherently very motivating. Hence, 90% of the learners found that the session was not infantilising but that it was rather enjoyable and not boring. All also highlighted the importance of the social link during the experience as a positive feature. Working in teams with a common goal (escaping the room) encourages participants to engage in the experience. The satisfaction of solving puzzles and the collaboration among teammates (encouragement, inspiration, etc.) also enhances this sense of motivation and boosts participants' self-confidence. Hence, participants not only had fun but also appreciated confronting good and bad practices in a realistic setting that everyone could relate to.

Secondly, as mentioned in the theoretical section of this research, learning is an active process that occurs through experiences, failures, and successes. It involves understanding how things work rather than passively learning elements without reflection. The escape game contextualizes important concepts, helping participants understand their relevance and importance. Additionally, the puzzles and challenges added an active component to the learning process. Moreover, adding a quiz at the end of the session confirms the concepts covered and proved to participants that they had learned something and were capable of adopting the right practices. Therefore, 100% argued that this session strengthened their capacities and 40% declared having learned new things.

Finally, unlike the other tested solutions, the escape game simulates a possible reality in which participants operate. This practical aspect in a safe environment boosts participants' confidence in their abilities, which can encourage them to adopt good practices in their daily lives. By giving the participants confidence in their abilities, we can also help them change their behavior. Thus, 60% felt more confident after the session, and 70% were motivated to change their behavior.

In conclusion, the Cyber Escape Game was ranked first place as the preferred solution by the participants. It appears to be an effective format as it adequately and with balance, addressed motivation, learning, and behavior. The inclusion of a quiz at the end of the session provided

significant added value, allowing participants to validate the knowledge gained during the session. This also boosted their self-confidence. In that respect, an Escape Game offers an immersive experience where participants must collaborate to achieve various objectives. Players are plunged into a realistic situation: their daily work environment. Consequently, they had to navigate between good and bad practices in the scenario to achieve their set objectives. This immersive format encourages players to engage and question themselves.

To conclude, this sub-section reviewed each tested solution individually and their results. Comments were added about the specificities of the solutions which could have influenced the answers of the participants. Therefore, the escape game was the preferred solution and the more traditional e-learning (Game 2C) was the least appreciated. Nevertheless, each solution had its specific features, sometimes resulting in unexpected outcomes. The following part will address a comparison of the efficacy of the solutions and will seek to verify the hypothesis while still considering the Constructivist Learning approach.

2. Evaluating the efficacy: comparison of the results

The previous analysis of the tested solutions highlighted the strong and weak features of each of the 5 tools. Each having its particularities, advantages and limits, participants gave different feedback. This part seeks to compare the results in order to address the effectiveness dimension at the core of this research. Which of these 5 solutions was and is the "most effective"? To assess the solutions, the method was influenced by the constructivist approach as developed in the methodology section. Then, in a second part, the hypotheses will be discussed, validated or refuted.

A. Assessing the results under the umbrella of the Constructivist Learning Theory

The participants ranked the cyber escape game in first place. But is this ranking true regarding with the global results and not just participants' rankings? Though it was the most popular solution to reach the top, the escape game might not be the most effective model as this research seeks to find. This section will explore and compare the results to find which of the 5 solutions is the closest to what can be considered as "the most effective" solution with regards to the constructivist learning theory's principles. In other words, which of the tested games integrates "active learning", "experiential learning" and "social integration" criteria still have good rates according to the participants' feedback. Firstly regarding the comparison of the results to the answers related to the assessment of motivation. The board games and the escape game received the highest positive rate with both 100% for the question related to enjoyment and similarly, none of the participants felt boredom during these

sessions. Regarding the three e-learnings, the ultra-gamified one had the more positive review. Hence, 67% answered “rather true” and 33% “completely true” while for the two other solutions, answers were more mixed. Additionally, with regard to the risk of infantilization, only the two gamified e-learning had positive answers with 58% for game B1 and 25% for game B2. Consequently, the board game and the escape game had the best results according to the participants’ surveys. This can be explained by the “active engagement” developed in the constructivist approach of learning. In both of these two solutions, learners had direct access to the knowledge through hands-on activities or problem-solving. Such methods are supposed to increase and enhance engagement, enjoyment and thus, motivation.

Secondly, the assessment of the learning prospects of each game is rather limited as it was not anchored in time or tested with assessments. Specific questions were asked to check if participants had learned new things and if they had strengthened the knowledge they already had. Hence, participants declared to have learned new things firstly with game B3, the traditional e-learning, with 75% positive answers, followed by game B2 et B1 (around 50%). The board game only accounts for 46% of “completely and rather true” while the escape game barely resembles 40%. However, when it comes to the question of reinforcing concepts already acquired, answers are similar to the motivation category. Thus, all the participants answered “completely true” or “rather true” regarding the escape game while for the board game, even if they also all answered positively, only 17% voted for the strongest positive affirmation and 67% for “rather true”. Nevertheless, the outcomes regarding the e-learning are also generally positive with a strong score for the traditional e-learning followed by game B2 and then B1. Only a few solutions included “experiential learning” which is about having direct experiences and real-world applications related to the studied notions. The traditional e-learning platform had parts of its courses related to “real-life” situations as it sought to spread awareness among employees about the good practices. Nevertheless, it seems that “experiential learning” was more developed in the escape game and partially with the board games which could explain the high scores regarding the reinforcement of prior knowledge. Such experiences enabled learners to confront their knowledge with real-life practice.

Thirdly, as with learning in the previous paragraph, assessing the change of behavior is difficult without long-term study. To assess it, participants were asked questions about their level of confidence in their skills and capacities, but also about their motivation to change their habits and adopt good cybersecurity practices. According to some of the principles of the constructivist learning theory, “social interaction” should enhance the learning process thanks to peer encouragement and inspiration which consequently influence the behavior. Nevertheless, the results tend to highlight the opposite. The three e-learning received the highest scores by the participants. For instance, game B1 was considered by 92% of the learners as a relevant solution to enhance confidence and motivation to

change their behavior while the results for the board game and the escape game were a bit lower, around 60 or 70% which still are high rand good esutls.

To summarize, the overall results are sometimes mixed and detached from the constructivist principles. The escape game seems to be the most appropriate solution to enhance motivation and engagement while for learning and behavior, gamified e-learning might be more suitable. Hence, the environment of learning appeared to be a key criteria influencing the results. Nevertheless, some limits must be recalled. Nonetheless, these results are not generalizable and will be discussed in more detail in the discussion section.

B. Answering the hypotheses

At the beginning of this research, four hypotheses were stated based on the general trends regarding gamification and serious games but also with respect to the theoretical framework. The previous parts of this section highlighted the advantages, disadvantages and global effectiveness of each solution. These parts bring key elements to validate or not the following hypotheses.

Hypothesis 1*: Gamified awareness sessions are more effective than traditional sessions in improving cybersecurity knowledge and behaviors.*

General trends, as highlighted in the literature review indeed indicate that gamified awareness sessions have more impact than the traditional. Nevertheless, the efficacy relies on the quality of the design. This was confirmed through this research as the escape game and the strongly gamified e-learning had the best scores and validated most of the criteria (motivation, learning and behavior). The element of comparison was the traditional e-learning which, surprisingly, still had great feedback. Hence, traditional and gamified methods should not be opposed. Maybe, the solution is somewhere in between, balancing between straight-forward methods with a more gamified approach in a secondary time.

Hypothesis 2*: Gamified solutions that include high motivational elements (e.g., rewards, challenges) are the most effective in engaging participants and improving learning outcomes.*

With regards to only the motivational elements, solutions including this type of elements indeed had higher effectiveness such as the escape game, or the strongly gamified e-learning. These elements such as a scoreboard and a cash price for the strongly gamified e-learning or the satisfaction of completing challenges with the escape game prove to be highly motivating.

Hypothesis 3*: Gamified solutions that incorporate diverse ways of learning (e.g., interactive tasks, simulations, multimedia) are the most effective in enhancing participants' understanding and retention of cybersecurity concepts.*

Only the escape game, the game B1 and, partially, the board game included various ways of learning. For instance, the Cyber Escape Game, which incorporated a variety of interactive tasks and realistic scenarios, was highly effective in enhancing understanding and retention. Participants reported strengthened knowledge (100%) and increased confidence (60%). Similarly, the fully gamified e-learning (Game B1) utilized multiple methods such as micro-sessions, challenges, and notes, which helped reinforce learning. Results of the board games are more mixed, which also reflects the more limited ways of learning included in the solution. Hence, the results indicate that the variety in learning methods could directly contribute to the effectiveness of the gamified solutions in imparting cybersecurity knowledge.

Hypothesis 4*: Gamified solutions that combine high motivational elements with diverse ways of learning are the most effective in improving cybersecurity knowledge, engagement, and behavior.*

Finally, regarding the last and fourth hypothesis, the link between motivational elements and the diverse ways of learning was supposed to enhance the efficacy of awareness sessions. The escape game goes along with the fourth hypothesis. It combined motivational elements such as team-based challenges and realistic scenarios with diverse learning methods like interactive puzzles and a follow-up quiz. This combination resulted in high engagement (90% enjoyment), effective learning (100% knowledge reinforcement), and positive behavioral intentions (70% motivation to change behavior). Similarly, the fully gamified e-learning (Game B1) also showed that combining motivational elements with diverse learning methods led to improved outcomes in all areas. However, some mixed results for certain questions regarding both solutions represent one of the limits to fully validating this hypothesis. Nevertheless, the evidence suggests that solutions incorporating both high motivational elements and diverse ways of learning, enhance cybersecurity awareness.

To sum up, the hypotheses have been partially validated, with some reservations. The first hypothesis is confirmed without, at the same time, discrediting the value of traditional methods. The second hypothesis is also validated as motivational elements were key shared elements for efficacy. However, hypotheses 3 and 4 need to be investigated in more detail. Although the overall results tend to confirm the hypotheses, some participants' feedback prevents their full validation.

Conclusion

To summarize the findings section, explored and analyzed the results of the research and answered the hypothesis. The Escape Game model emerged as the most effective gamified solution, within the limits of this research, balancing high motivation, educational impact, and behavioral change, and aligning with the principles of the constructivist learning theory. However, other types of gamified solutions underlined positive results and should be considered for further research. For instance, the fully gamified e-learning solution also showed significant effectiveness, particularly regarding behavior change, but educational outcomes were more moderate. The traditional non-gamified e-learning had strong educational results but lacked engagement, and the partially gamified e-learning faced criticism for its limited motivational appeal. Overall, the effectiveness of gamified solutions depends significantly on their design quality, the inclusion of diverse learning methods, and motivational elements. Additionally, the first and second hypotheses were all validated unlike the two others which need to be further investigated.

Discussion

This research aimed to assess different gamified solutions to find which type and format could represent a suitable alternative to traditional methods for spreading cybersecurity awareness. This section's goal is to summarize and interpret the results and to additionally consider the implications and limitations. Finally, the last section will provide recommendations regarding the research question and further research on this topic.

The findings highlighted different insights to answer the research question: Which type of gamified solution is the most effective to raise cyber awareness? As discussed earlier, the Escape Game emerged as an effective tool, aligning with the constructivist learning principles of active and experiential learning. Participants showed high levels of engagement, strengthened their knowledge, and felt more confident in their cybersecurity practices. Additionally, game B1, the ultra-gamified e-learning, also demonstrated strong results, particularly in terms of motivation and behavior change. The inclusion of high motivational elements such as competitions and rewards appeared to be key factors in sustaining engagement and encouraging positive cybersecurity behaviors. In contrast, the traditional e-learning (Game B3) and partially gamified e-learning (Game B2) platforms were effective in reinforcing knowledge but lacked the motivational elements and diverse learning methods that contribute to a more comprehensive learning experience. The board game, despite being enjoyable, had limitations in motivating behavior change and balancing learning with engagement.
Beyond these results, the impact of the learning environment on motivation, learning, and behavior was highlighted. Participants using e-learnings platforms were directly confronted with learning and knowledge as the initial purpose of this format. In contrast, with serious games such as board games and escape games, learners might not directly understand what and how they are learning due to the non-traditional learning environment. This environmental factor likely influenced the observed results across all categories. Interestingly, e-learnings received surprisingly high feedback for behavior change, demonstrating their effectiveness in traditional knowledge transfer settings. It stresses that traditional and gamified methods should be balanced.

Additionally, several limitations of this research must be highlighted. As discussed in the methodology section, these outcomes should not be generalized. The study was conducted over a short period with a small population sample, which does not capture the possible long-term impacts and efficacy of these solutions. Moreover, the reliance on self-reported data through surveys could introduce bias, as participants might overestimate their engagement and learning outcomes. Future research should address these limitations by employing larger samples, longitudinal designs, and objective measures of behavior change and learning.

Finally, based on the findings and their analysis, several recommendations can be made. It is suggested to include these concepts in a more general strategy for cybersecurity awareness. For instance, the first step could be to secure and strengthen the fundamental principles of cybersecurity with a traditional method, similar to Game B3. Subsequently, it would be advisable to continue stimulating and enhancing this knowledge through a slightly more gamified e-learning platform, avoiding redundancy, as seen with games B1 or B2. Finally, integrating more original and dynamic sessions, such as a board game or an escape game, occasionally would be beneficial.

This strategic approach offers a comprehensive long-term solution that should promote sustainable learning without generating frustration or other negative feelings towards cybersecurity among participants. As highlighted by the constructivist learning approach, a strategy over time is important, as knowledge is an active process made of experiences. It requires time and repetition for learners to assimilate and accommodate new perceptions of the world. Hence, the results suggest that a hybrid approach, combining traditional methods with gamified elements, might offer a balanced solution. Traditional e-learning can effectively deliver clear and structured content, while gamified elements can boost engagement and motivation.

Conclusion

This research aimed to identify which format of gamified awareness solution could be the most effective regarding the motivation, learning and behavior criterias. Using a semi-experimental design and surveys to collect quantitative data from participants, it can be concluded that the design elements, the environment and engagement strategies significantly influence the effectiveness of these solutions. The results indicate that participants are more receptive to gamified solutions that incorporate interactive tasks, team-based challenges, realistic scenarios, and those that provide immediate feedback and rewards.

Hence, to answer the research question: Which type of gamified solution is the most effective to raise cyber awareness? The escape game and the ultra-gamified solutions appear to be the most effective if we consider participants' feedback and the design of these solutions.

The findings were based on three criteria: motivation, learning, and behavior. While the escape game and the board game scored highest for motivation, the e-learnings were surprisingly higher rated for learning and behavior. This highlights the importance of the learning environment and the methods through which knowledge is imparted. Consequently, a comprehensive 360° strategy for cybersecurity awareness is proposed, combining traditional and gamified methods to achieve strong long-term effects.

In conclusion, gamification and serious games represent a relevant alternative to the traditional methods. Nevertheless, their efficacy depends on several criteria including their design and the environment within which they are used. The escape game was found to be one of the most efficient solutions as it proposed a complete experience with teamwork, hand-on enigmas, problem solving while at the same time, spreading awareness about good and bad practices in cybersecurity. Additionally, game B1, the ultra-gamified e-learning also represents an effective alternative as underlined the findings.

Finally, this master’s thesis addressed an international security issue related to human behavior. It proposed a way to improve cybersecurity awareness in order to enhance a so-called “human firewall”. Cybersecurity is a global challenge as it concerns every organization, countries and citizens but also every domain. The democratization of computers and information systems makes this topic highly sensitive as reminded of the recent “Crowdstike” incident, blocking millions of computers and dozens of airports throughout the world. Though it seems to only be a technical issue, systems vulnerabilities and breaches are discovered every day causing more or less risks. In a world with rising tensions, conflicts and intolerance, cybersecurity plays a sometimes underestimated importance. Hence its risks must be globally mitigated, including the human role.

Bibliography

Ajzen, Icek. “The Theory of Planned Behavior.” *ORGANIZATIONAL BEHAVIOR AND HUMAN DECISION PROCESSES*, vol. 50, 1991, pp. 179–211.

---. “The Theory of Planned Behavior: Selected Recent Advances and Applications.” *Europe’s Journal of Psychology*, vol. 16, no. 3, 2020, pp. 352–56, https://doi.org/10.5964/ejop.v16i3.3107.

Al-Daeef, et al. “Security Awareness Training: A Review.” *Proceedings of the World Congress on Engineering*, vol. 1, 2017.

Alotaibi et al. “A Review of Using Gaming Technology for Cyber-Security Awareness.” *International Journal for Information Security Research*, vol. 6, no. 2, 2016.

Aloul, A. Fadi. “The Need for Effective Information Security Awareness.” *Journal of Advanced in Information Technology*, vol. 3, no. 3, 2012, https://doi.org/10.4304/jait.3.3.176-183.

Alruwaili, Ahmed. “A Review of the Impact of Training on Cybersecurity Awareness.” *International Journal of Advanced Research in Computer Science*, vol. 10, no. 5, 2019, https://doi.org/10.26483/ijarcs.v10i5.6476.

Alvarez, Edgar. “Sony Pictures Hack: The Whole Story.” *Engadget*, 10 Dec. 2014, https://www.engadget.com/2014-12-10-sony-pictures-hack-the-whole-story.html?guccounter=1.

Ani et al. *Human Capability Evaluation Approach for Cyber Security in Critical Industrial Infrastructure*. Springer, 2016, p. 170, https://doi.org/DOI 10.1007/978-3-319-41932-9_14.

Bada, Maria, et al. “Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?” *International Conference on Cyber Security for Sustainable Society*, 2015.

Bada, Steve Olusegun. “Constructivism Learning Theory: A Paradigm for Teaching and Learning.” *Journal of Research & Method in Education*, vol. 5, no. 6, 2015, pp. 67–70, https://doi.org/10.9790/7388-05616670.

Bandura, Albert. “Self-Efficacy: Toward a Unifying Theory of Behavioral Change.” *Advances in Behaviour Research and Therapy*, vol. 1, no. 4, 1978, pp. 139–61.

Baptista, and Oliviera. “Gamification and Serious Games: A Literature Meta-Analysis and Integrative Model.” *Computers in Human Behavior*, vol. 92, 2019, pp. 306–15, https://doi.org/10.1016/j.chb.2018.11.030.

Baral, and Arachchilage. “Building Confidence Not to Be Phished through a Gamified Approach: Conceptualising User’s Self-Efficacy in Phishing Threat Avoidance Behaviour.” *9 Cybersecurity and Cyberforensics Conference (CCC)*, 2019, https://doi.org/10.1109/CCC.2019.000-1.

Bellotti et al. “Assessment in and of Serious Games: An Overview.” *Hindawi Publishing Corporation*, vol. 2013, 2013, pp. 1–11, https://doi.org/10.1155/2013/136864.

Bereiter. “Constructivism, Socioculturalism, and Popper’s World.” *Educational Researcher*, vol. 23, no. 7, 1994, pp. 21–23.

Brookes, Elisabeth. “The Theory Of Planned Behavior: Behavioral Intention.” *SimplyPsychology*, 11 Oct. 2023, https://www.simplypsychology.org/theory-of-planned-behavior.html.

Buckley, Patrick, and Elaine Doyle. “Gamification and Student Motivation.” *Interactive Learning Environments*, vol. 24, no. 6, 2016, pp. 1162–75, https://doi.org/10.1080/10494820.2014.964263.

Burgess, Matt. “Conti’s Attack Against Costa Rica Sparks a New Ransomware Era.” *Wired*, 12 June 2022, https://www.wired.com/story/costa-rica-ransomware-conti/.

Capelle, Pierre, and Philippe Trouchaud. *Baromètre Data Breach: Violation des données personnelles, quelle gestion du risque ?* 2020, https://www.pwc.fr/fr/publications/data/barometre-data-breach.html#cta-1.

Chourci, Nazli, and David D. Clark. *International Relations in the Cyber Age: The Co-Evolution Dilemma*. MIT Presse, 2018.

Clark, David, et al. *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*. National Academies Press, 2014.

Creswell, John W. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. Sage, 2014, https://archive.org/details/methodology-alobatnic-libraries-creswell/page/n4/mode/1up.

Davies, Josh. "Why Are Humans the Weakest Link in Cybersecurity?" *Alert Logic*, 5 July 2023, https://www.alertlogic.com/blog/why-humans-weakest-link-cybersecurity/.

de Bruijn, and Janssen. "Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies." *Government Information Quarterly*, vol. 34, 2018, pp. 1–7, https://doi.org/10.1016/j.giq.2017.02.007.

Deterding et al. *From Game Design Elements to Gamefulness: Defining "Gamification."* 2011, https://doi.org/10.1145/2181037.2181040.

Dzuba, Elaine, and Juliette Cash. "Introducing Cloudflare's 2023 Phishing Threats Report." *Cloudflare Blog*, 16 Aug. 2023, https://blog.cloudflare.com/2023-phishing-report/.

Eszter Diana Oroszi. "Using Gamification to Improve the Security Awareness of Users: The Security Awareness Escape Room." *ISACA*, vol. 4.

FBI. "Update on Sony Investigation." *FBI*, 19 Dec. 2014, https://fbi.gov/news/press-releases/update-on-sony-investigation.

Featherly, Kevin. "Neuromancer." *Britannica*, 26 July 2024, https://www.britannica.com/topic/Neuromancer.

Glorin, Sebastian, and Phanindra Kolluru. “Rethinking the Weakest Link in the Cybersecurity Chain.” *ISACA*, vol. 5, 2021, https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/rethinking-the-weakest-link-in-the-cybersecurity-chain.

Greene. “Kevin Mitnick Was No Hacker.” *The Register*, 2 Mar. 2000, https://www.theregister.com/2000/03/02/kevin_mitnick_was_no_hacker/.

Guay, Frédéric. “Applying Self-Determination Theory to Education: Regulations Types, Psychological Needs, and Autonomy Supporting Behaviors.” *Canadian Journal of School Psychology,* vol. 37, no. 1, 2022, pp. 75–92, https://doi.org/10.1177/08295735211055355.

Gwenhure, and Rahayu. “Gamification of Cybersecurity Awareness for Non-IT Professionals: A Systematic Literature Review.” *International Journal of Serious Games*, vol. 11, no. 1, 2024, https://doi.org/10.17083/ijsg.v11i1.719.

Hakmeh, Joyce, et al. “What Is a Cyberattack?” *Chatham House*, 18 Feb. 2022, https://www.chathamhouse.org/2022/02/what-cyber-attack.

Hamari et al. “Does Gamification Work? — A Literature Review of Empirical Studies on Gamification.” *Hawaii International Conference on System Science*, vol. 47, 2014, https://doi.org/10.1109/HICSS.2014.377.

Hammady, Ramy, and Sylvester Arnab. “Serious Gaming for Behaviour Change: A Systematic Review.” *Information*, vol. 13, no. 3, 2022, https://doi.org/10.3390/info13030142.

Hart et al. “Riskio: A Serious Game for Cyber Security Awareness and Education.” *Computers & Security*, vol. 95, 2020, https://doi.org/10.1016/j.cose.2020.101827.

IBM. “Qu’est-Ce Qu’une Attaque Par Hameçonnage ?” *IBM*, https://www.ibm.com/fr-fr/topics/phishing. Accessed 23 June 2024.

Joint Task Force Transformation Initiative. “NIST SP 800-39: Managing Information Security Risk: Organization, Mission, and Information System View.” *NIST*, 2011, https://doi.org/10.6028/NIST.SP.800-39.

Jonassen et al. *Learning to Solve Problems with Technology : A Constructivist Perspective*. 2nd ed., Merrill Prentice Hall, 1999, https://archive.org/details/learningtosolvep00jona.

Karagiorgas, and Niemann. “Gamification and Game-Based Learning.” *Journal of Educational Technology Systems*, vol. 54, no. 4, 2016, pp. 499–519, https://doi.org/10.1177/0047239516665105.

Keller, John. “Development and Use of the ARCS Model of Instructional Design.” *Journal of Instructional Development*, 1987.

---. “Motivation, Learning, and Technology: Applying the ARCS-V Motivation Model.” *Participatory Educational Research*, vol. 3, no. 2, 2016, https://doi.org/10.17275/per.16.06.3.2.

Kolb, David. “The Process of Experiential Learning.” *Experiential Learning: Experience As The Source Of Learning And Development*, 1984.

Krath, et al. “Revealing the Theoretical Basis of Gamification: A Systematic Review and analysis of Theory in Research on Gamification, Serious Games and game-Based Learning.” *Computers in Human Behavior*, vol. 125, 2021, https://doi.org/10.1016/j.chb.2021.106963.

Laamarti et al. “An Overview of Serious Games.” *International Journal of Computer Games Technology*, vol. 2014, no. 1, 2014, https://doi.org/10.1155/2014/358152.

Landers et al. “Gamification Science, Its History and Future: Definitions and a Research Agenda.” *Simulation & Gaming*, vol. 49, no. 3, 2018, pp. 315–37, https://doi.org/10.1177/1046878118774385.

MacAskill, Ewen. “Major Cyber-Attack on UK a Matter of ‘when, Not If’ – Security Chief.” *The Guardian*, 23 Jan. 2018, https://www.theguardian.com/technology/2018/jan/22/cyber-attack-on-uk-matter-of-when-not-if-says-security-chief-ciaran-martin.

Makdech, Kocila, and Marie-Violette Bernard. “Comment la Corée du Nord a pu pirater Sony Pictures.” *Franceinfo*, 16 2014, https://www.francetvinfo.fr/culture/cinema/piratage-de-sony/la-coree-du-nord-est-a-l-origine-du-piratage-de-sony-pictures-selon-l-enquete-officielle-des-etats-unis_777191.html.

MediaPRO. *State of Privacy and Security Awareness Report*. 2020, https://www.bsigroup.com/globalassets/localfiles/en-ie/our-services/mediapro/2020_state_of_privacy-security_awareness_report_mediapro.pdf.

Microsoft. “Qu’est-Ce Que La Compromission de Messagerie d’entreprise (BEC) ?” *Microsoft*, https://www.microsoft.com/fr-fr/security/business/security-101/what-is-business-email-compromise-bec. Accessed 21 Apr. 2024.

Morgan, Steve. “Cybercrime To Cost The World 8 Trillion Annually In 2023.” *Cybercrime Magazine*, 17 Oct. 2022, https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/.

Mouaheb, Houda, et al. “The Serious Game: What Educational Benefits?” *Procedia, Social and Behavioral Sciences*, vol. 46, 2012, pp. 5502–08, https://doi.org/10.1016/j.sbspro.2012.06.465.

Mueller et al. “Cyber Operations during the Russo-Ukrainian War.” *CSIS*, 13 July 2023, https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.

Paquay, Maxime. “Piratage de Sony: de la cyberattaque au cyberterrorisme.” *RTBF*, 18 Dec. 2012, https://www.rtbf.be/article/piratage-de-sony-de-la-cyberattaque-au-cyberterrorisme-8603146.

Ponton & Rhea. “Autonomous Learning from a Social Cognitive Perspective.” *New Horizons in Adult Education and Human Resource Development*, vol. 20, no. 2, 2013, pp. 38–49, https://doi.org/10.1002/nha3.10250.

Price, Rob. “Sony Hackers Threaten Terror Attack over ‘The Interview.’” *Daily Dot*, 16 Dec. 2021, https://www.dailydot.com/debug/sony-gop-the-interview-terrorist-attack-threat/.

Qi Zhang, and Zhonggen Yu. “Investigating and Comparing the Effects on Learning Achievement and Motivation for Gamification and Game-Based Learning: A Quantitative Study Employing Kahoot.” *Education Research International*, 2022, p. 16, https://doi.org/10.1155/2022/9855328.

Reffgen, Cartsen. “Protection Goals: CIA and CIAA.” *EOS*, 25 July 2018, https://eosgmbh.com/en/protection-goals-cia-and-ciaa.

Reuters. “Cyber Attack on Costa Rica Grows as More Agencies Hit, President Says.” *Reuters*, 17 May 2022, https://www.reuters.com/world/americas/cyber-attack-costa-rica-grows-more-agencies-hit-president-says-2022-05-16/.

Rieff, Iris. *Systematically Applying Gamification to Cyber Security Awareness Trainings A Framework and Case Study Approach*. TU Delft, https://repository.tudelft.nl/record/uuid:bf832ca0-91d9-4be1-9a25-fe284c23d115.

Rieß-Marchive, Valéry. “Le phishing, impliqué dans l’attaque de Sony Pictures.” *LeMagIT*, 24 Apr. 2015,

https://www.lemagit.fr/actualites/4500244982/Le-phishing-implique-dans-lattaque-de-Sony-Pictures.

Saalman, Lora, et al. *Cyber Posture Trends in China, Russia, The United States and the European Union*. Stockholm International Peace Research Institute, Dec. 2022, pp. 9–12, https://www.sipri.org/sites/default/files/2022-12/2212_cyber_postures_0.pdf#:~:text=URL%3A%20https%3A%2F%2Fwww.sipri.org%2Fsites%2Fdefault%2Ffiles%2F2022.

Sailer et al. "How Gamification Motivates: An Experimental Study of the Effects of Specific Game Design Elements on Psychological Need Satisfaction." *Computers in Human Behavior*, vol. 69, 2016, pp. 371–80, https://doi.org/10.1016/j.chb.2016.12.033.

Sharif, and Ameen. "A Review on Gamification for Information Security Training." *International Conference of Modern Trends in Information and Communication Technology Industry*, 2021.

"The Etymology of 'Cyberspace' (n.)." *Online Etymology Dictionary*, https://www.etymonline.com/word/cyberspace. Accessed 23 Mar. 2024.

"The Weakest Link: If Only Computer Security Did Not Have to Involve People." *The Economist*, 26 Oct. 2002, https://www.economist.com/special-report/2002/10/26/the-weakest-link.

Thrive DX. *2022 Global Cybersecurity Awareness Training Study*. Aug. 2022, https://thrivedx-2714581.hs-sites.com/cyber-security-awareness-study-download-0.

Toth, Patricia, and Penny Klein. "A Role-Based Model for Federal Information Technology/ Cybersecurity Training." *NIST Special Publication*, vol. 800, no. 16, 2014.

Ullah et al. "Serious Games in Science Education: A Systematic Literature Review." *Virtual Reality & Intelligent Hardware*, vol. 4, no. 3, 2022, pp. 189–209, https://doi.org/10.1016/j.vrih.2022.02.001.

Verizon. *2024 Data Breach Investigations Report*. 2024, https://www.verizon.com/business/resources/reports/dbir/.

Vygotskii. *Mind in Society : The Development of Higher Psychological Processes*. Harvard University Press, 1978.

"What Is a Cyberattack?" *IBM*, https://www.ibm.com/topics/cyber-attack.

WikiLeaks. "Sony." *WikiLeaks*, 16 Apr. 2015, https://wikileaks.org/sony/press/.

Wolfenden, Brad. "Gamification as a Winning Cyber Security Strategy." *Computer Fraud & Security*, 2019.

Zhonggen, Yu. "A Meta-Analysis of Use of Serious Games in Education over a Decade." *International Journal of Computer Games Technology*, vol. 2019, 2019, p. 8, https://doi.org/10.1155/2019/4797032.

Zwilling et al. "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study." *Journal of Computer Information Systems*, vol. 62, no. 1, 2020, pp. 82–97, https://doi.org/10.1080/08874417.2020.1712269.

Annexes

Annexe n°1 *- Consent agreement for study participation in french and translated in english*

Annexe n°2 *- Overview of the results of the post-test surveys (in french)*

Annexe n°3 *- Overview of the results of the post-test surveys (translated from french in english)*

Annexes n°2 and n°3 represent a table summarizing the surveys' questions. Each line summarizes statements which were more developed and contextualized in the survey. For practical reasons and software limitations, they were summarized in a shortened statement. To each of these statements, participants had to choose between four answers: "Completely wrong, rather wrong, rather true, completely true".

Annexes n°1 - Consent agreement for study participation in french and translated in english

ORIGINAL (FRENCH): FORMULAIRE D'INFORMATION ET DE CONSENTEMENT

Je, soussigné, [Nom, Prénom] déclare accepter, librement et de façon éclairée, de participer comme sujet à l'étude intitulée : « Le marché et les enjeux de la gamification cyber ».

Sous la direction de :

- [redacted]([redacted])
- David ERKOMASHVILI (Charles University)

Investigateur principal : Adèle Brunagel (Stagiaire GRC chez [redacted] et étudiante en M2 à la Charles University)

But de l'étude : L'étude a pour finalité d'étudier la question suivante : « Quel format de sensibilisation gamifié est-il le plus efficace ? ». Cette étude cherche donc à étudier les effets que peuvent avoir les concepts de « gamification » et « serious game » sur le comportement et l'apprentissage des participants. Il s'agira aussi d'étudier les plusieurs types de jeux proposés, leurs avantages et inconvénients pour pouvoir permettre à [redacted] de se faire un avis sur ce type d'offres.

Raison et nature de la participation : Votre participation sera requise pour 3 ou 4 rencontres entre avril et juillet. Ces sessions dureront **entre 30 min et 1h30 maximum**. Elles auront lieu dans les locaux [redacted] à Sèvres en fonction de vos disponibilités. Vous aurez à répondre à **un questionnaire** se rapportant au jeu testé **après chaque session**. Vous aurez aussi à remplir **deux questionnaires supplémentaires**, un premier avant le début des sessions (celui-ci), et un dernier quelque temps après la dernière session. Si nécessaire, le participant est libre de demander plus d'information

Avantages pour le participant : Bien que vous ne retirerez aucun avantage direct à participer à ce projet de recherche, votre implication nous est plus qu'utile pour mieux comprendre l'efficacité et l'intérêt des serious game et de la gamification. De plus, l'expérience devrait être relativement agréable, comme il s'agit principalement de tester plusieurs jeux.

Inconvénients pour le participant : Votre participation à cette étude ne devrait pas comporter d'inconvénients significatifs, si ce n'est le fait de donner un peu de votre temps pour participer aux différentes sessions mais aussi pour répondre aux plusieurs questionnaires. Toutefois, il est important de noter que sur les 3/4 sessions, **toutes ne dureront pas plus d'une heure**, et les **questionnaires** resteront relativement **court**, c'est-à-dire **moins de 5 minutes**.

Liberté du participant : Votre **participation à ce projet de recherche est volontaire**. Vous êtes donc **libre de refuser d'y participer**. Vous pouvez également vous retirer de ce projet de recherche à n'importe quel moment, sans avoir à donner de raisons, en informant la chercheuse responsable ou un membre de l'équipe de recherche.

Si vous décidez de vous retirer :

- Cela n'impactera pas les relations avec les différents membres de l'entreprise.
- Vos informations seront gardées mais pourront être supprimées à votre demande

Engagement de l'investigateur principal : L'investigateur principal (Adèle BRUNAGEL) ainsi que le reste du groupe de recherche ([redacted] et David ERKOMASHVILI) s'engagent à mener cette recherche selon les dispositions éthiques et déontologiques, à protéger l'intégrité physique, psychologique et sociale des personnes tout au long de la recherche et à assurer la confidentialité des informations recueillies.

Confidentialité des informations :

- Les informations collectées seront anonymisées et votre identité ne sera pas révélée dans l'analyse de l'étude.
- Toutefois, si vous le souhaitez, vous avez **la possibilité de remplir les questionnaires de cette étude anonymement.** Il vous faudra cependant vous assurer de trouver un pseudo ne révélant pas votre identité et que vous utiliserez à chaque session. Il reste aussi possible **de participer avec votre prénom et nom.**
- Il est important pour le bon fonctionnement de cette étude d'avoir un suivi des réponses individuelles des participants au fur et à mesure des sessions. C'est pour cela qu'il vous faudra choisir entre répondre anonymement aux questionnaires ou bien avec votre véritable identité.

Possibilité de commercialisation : Nulle

Déontologie et éthique : Confidentialité et informations personnelles seront préservée.

Conflit d'intérêt : Aucun conflit d'intérêt n'a été mis en avant.

Coordonnées de personnes-ressources : Si vous avez des questions ou éprouvez des problèmes reliés au projet de recherche, ou si vous souhaitez vous en retirer, vous pouvez communiquer l'équipe de recherche par Teams ou par mail.

- Adèle BRUNAGEL : abrunagel@[redacted]
- [redacted]: [redacted]

ENGLISH VERSION: INFORMATION AND CONSENT FORM

I, the undersigned, [Name, First Name], hereby declare my free and informed consent to participate as a subject in the study entitled: "The Market and Challenges of Cyber Gamification."

Under the direction of:

- [redacted] ([redacted])
- David ERKOMASHVILI (Charles University)

Principal Investigator:

- Adèle Brunagel (GRC intern at [redacted] and student in M2 at Charles University)

Purpose of the study: The study aims to explore the following question: "**Which type of gamified solution is the most effective to raise cyber awareness?**" This study seeks to examine the effects of the concepts of "gamification" and "serious games" on participants' behavior and learning. It will also investigate the various types of games offered, their advantages and disadvantages, to enable [redacted] to form an opinion on this type of offering.

Reason and nature of participation: Your participation will be required for 3 or 4 meetings between April and July. These sessions will last between 30 minutes and a maximum of 1 hour and 30 minutes. They will take place at [redacted] premises in Sèvres based on your availability. You will need to complete a questionnaire related to the tested game after each session. You will also have to complete two additional questionnaires, one before the start of the sessions (this one), and another some time after the last session. If necessary, participants are free to request more information.

Benefits for the participant: Although you will not receive any direct benefits from participating in this research project, your involvement is invaluable in helping us better understand the effectiveness and interest of serious games and gamification. Additionally, the experience should be relatively enjoyable, as it mainly involves testing various games.

Disadvantages for the participant: Your participation in this study should not entail significant disadvantages, except for the time you will need to spend participating in the various sessions and answering the questionnaires. However, it is important to note that out of the 3/4 sessions, not all will st more than an hour, and the questionnaires will remain relatively short, i.e., less than 5 minutes.

Participant's freedom: Your participation in this research project is voluntary. Therefore, you are free to refuse to participate. You can also withdraw from this research project at any time without giving any reasons, by informing the responsible researcher or a member of the research team.

If you decide to withdraw:

- This will not affect relationships with different members of the company.
- Your information will be retained but can be deleted at your request.

Commitment of the principal investigator: The principal investigator (Adèle BRUNAGEL) and the rest of the research team ([redacted] [redacted]et David ERKOMASHVILI) commit to conducting this research according to ethical and deontological provisions, protecting the physical, psychological, and social integrity of the participants throughout the research, and ensuring the confidentiality of the information collected.

Confidentiality of information:

- The collected information will be anonymized, and your identity will not be revealed in the study analysis.
- However, if you wish, you can fill out the study questionnaires anonymously. You will need to ensure you find a pseudonym that does not reveal your identity and use it for each session. It is also possible to participate with your first and last name.
- It is important for the smooth functioning of this study to have individual response tracking of participants throughout the sessions. Therefore, you will need to choose between responding anonymously to the questionnaires or using your real identity.

Commercialization possibility: None

Deontology and ethics: Confidentiality and personal information will be preserved.

Conflict of interest: No conflict of interest has been highlighted.

Contact information for resource persons: If you have any questions or encounter any problems related to the research project, or if you wish to withdraw, you can contact the research team via Teams or email.

- Adèle BRUNAGEL : abrunagel@[redacted]
- [redacted]: [redacted]

Annexes n°2 - Overview of the results of the post-test surveys (in french)

Thème	Questions	Board game	2.1	2.2	2.3	Escape Game	Board game	2.1	2.2	2.3	Escape Game	Board game	2.1	2.2	2.3	Escape Game	Board game	2.1	2.2	2.3	Escape Game
		Complétement faux					Plutôt faux					Plutôt vrai					Complètement vrai				
Motivation	Je me suis amusé,e	0%	0%	8%	25%	0%	0%	0%	33%	42%	0%	27%	67%	33%	33%	40%	73%	33%	25%	0%	60%
Motivation	Je me suis ennuyé,e	100%	42%	42%	8%	90%	0%	58%	58%	50%	10%	0%	0%	0%	17%	0%	0%	0%	0%	25%	0%
Motivation	Renforcement du teambuilding	0%	N/A	N/A	N/A	0%	6%	N/A	N/A	N/A	0%	33%	N/A	N/A	N/A	30%	60%	N/A	N/A	N/A	70%
Motivation	J'ai trouvé que c'était infantilisant,	90%	42%	17%	N/A	90%	10%	33%	25%	N/A	0%	0%	25%	50%	N/A	10%	0%	0%	8%	N/A	0%
Motivation	Je n'ai pas décroché pendant la session	80%	N/A	N/A	N/A	0%	20%	N/A	N/A	N/A	20%	0%	N/A	N/A	N/A	40%	0%	N/A	N/A	N/A	40%
Learning	J'ai renforcé mes connaissances	7%	17%	8%	8%	¨0%	13%	17%	25%	0%	0%	67%	50%	42%	58%	50%	13%	17%	25%	33%	50%
Learning	J'ai appris de nouvelles choses	33%	17%	25%	17%	20%	20%	33%	35%	8%	40%	33%	42%	17%	50%	40%	13%	8%	33%	25%	0%
Behavior	Cette session m'a motivé à changer de comprotement vis-à-vis des bonnes pratiques en cybersécurité,	27%	0%	8%	0%	20%	33%	8%	25%	8%	¨10%	40%	75%	42%	33%	50%	0%	17%	25%	58%	20%
Behavior	J'ai plus confiance en mes connaissances et compétences	20%	0%	0%	8%	0%	20%	8%	0%	0%	40%	60%	75%	50%	58%	50%	0%	17%	50%	33%	10%
Solution (tool)	J'ai trouvé que c'était facile d'utilisation, J'ai trouvé que c'était facile à comprendre	0%	0%	0%	8%	0%	7%	0%	17%	8%	10%	67%	67%	8%	50%	60%	26%	33%	75%	33%	30%
Solution (tool)	J'ai apprécié y jouer/tester,	0%	0%	8%	42%	0%	0%	8%	33%	33%	0%	26%	58%	25%	25%	30%	73%	33%	33%	0%	70%
Solution (tool)	J'ai trouvé que cette solution proposé quelque chose d'innovant et d'utile	20%	8%	0%	17%	0%	33%	8%	33%	58%	0%	27%	50%	42%	25%	30%	20%	33%	25%	0%	70%

Annexes n°3 - Overview of the results of the post-test surveys (translated from french in english)

Theme	Questions	Board game	B2	B1	B3	Escape Game	Board game	B2	B1	B3	Escape Game	Board game	B2	B1	B3	Escape Game	Board game	B1	B2	B3	Escape Game
		Completely false					Rather false					Rather true					Compeltely true				
Motivation	I had fun/enjoyed	0%	0%	8%	25%	0%	0%	0%	33%	42%	0%	27%	67%	33%	33%	40%	73%	33%	25%	0%	60%
Motivation	I was bored	100%	42%	42%	8%	90%	0%	58%	58%	50%	10%	0%	0%	0%	17%	0%	0%	0%	0%	25%	0%
Motivation	Teambuilding reinforcement	0%	N/A	N/A	N/A	0%	6%	N/A	N/A	N/A	0%	33%	N/A	N/A	N/A	30%	60%	N/A	N/A	N/A	70%
Motivation	I found it infantilising,	90%	42%	17%	N/A	90%	10%	33%	25%	N/A	0%	0%	25%	50%	N/A	10%	0%	0%	8%	N/A	0%
Motivation	I didn't lose interest during the session	80%	N/A	N/A	N/A	0%	20%	N/A	N/A	N/A	20%	0%	N/A	N/A	N/A	40%	0%	N/A	N/A	N/A	40%
Learning	I reinforced my knowledge	7%	17%	8%	8%	0%	13%	17%	25%	0%	0%	67%	50%	42%	58%	50%	13%	17%	25%	33%	50%
Learning	I learned new things	33%	17%	25%	17%	20%	20%	33%	35%	8%	40%	33%	42%	17%	50%	40%	13%	8%	33%	25%	0%
Behavior	This session motivated me to change my attitude to good cyber security practice,	27%	0%	8%	0%	20%	33%	8%	25%	8%	¨10%	40%	75%	42%	33%	50%	0%	17%	25%	58%	20%
Behavior	I'm more confident in my knowledge and skills	20%	0%	0%	8%	0%	20%	8%	0%	0%	40%	60%	75%	50%	58%	50%	0%	17%	50%	33%	10%
Solution (tool)	I found it easy to use, I found it easy to understand	0%	0%	0%	8%	0%	7%	0%	17%	8%	10%	67%	67%	8%	50%	60%	26%	33%	75%	33%	30%
Solution (tool)	I enjoyed playing/testing it,	0%	0%	8%	42%	0%	0%	8%	33%	33%	0%	26%	58%	25%	25%	30%	73%	33%	33%	0%	70%
Solution (tool)	I found that this solution offered something innovative and useful	20%	8%	0%	17%	0%	33%	8%	33%	58%	0%	27%	50%	42%	25%	30%	20%	33%	25%	0%	70%