TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Timm Jeff E. Luyten 184561IVCM

RAISING CYBER AWARENESS WITH NON-IT PROFESSIONALS WORKING IN A HOME OFFICE ENVIRONMENT USING A PILOT VIDEO GAME CONCEPT

Master's Thesis

Supervisor: Birgy Lorenz PhD
Cyber Security

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia Teaduskond

Timm Jeff E. Luyten 184561IVCM

KÜBERTEADLIKKUSE SUURENDAMINE TÖÖTAJATE HULGAS, KES POLE IT-PROFESSONAAL JA KES TÖÖTAB KAUGTÖÖL, LÄBI VIDEOMÄNGU IDEEKAVA

Magistritöö

Juhendaja: Birgy Lorenz PhD
Küberturvalisus

Tallinn 2020

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Timm Jeff E. Luyten

01.02.2020

Abstract

The covid-19 outbreak in 2020 has had a big impact in society forcing employees to work remotely from home. Cyber security while normally controlled in a business environment must now be managed remotely in different environments that introduce different vulnerabilities to be tackled. While it is well known that humans are the weak link in cyber security, additional home office cyber security risks are exposed. In this thesis cyber awareness trainings are analyzed, and educational models and individual elements are researched to support a cyber awareness video game training method. Using video games as a learning medium does not come without its challenges; the thesis researches possible solutions to those challenges and analyses some of the more popular cyber training games to gather ideas for the pilot game. A survey is done to the focus group of secretaries to gather crucial information on their IT competence, awareness trainings, and cyber security confidence levels. Additionally, the data is used to extract elements for the pilot game structure. The pilot game contains core elements such as a story, learning and motivational mechanics, art style and scenarios.

This thesis is written in English and is 96 pages long, including 11 chapters, 13 figures, 2 appendixes and 137 references.

Annotatsioon

Covid-19 puhang 2020. aastal on ühiskonnale suurt mõju avaldanud, sundides töötajaid kodus töötama. Küberjulgeolekut, mida tavaliselt kontrollitakse ärikeskkonnas, tuleb nüüd juhtida kaugjuhtimisega erinevates keskkondades, mis toob esile erinevaid nõrki kohti. On teada, et inimesed on küberturvalisuse nõrk lüli, aga lisaks sellele ilmnevad nüüd veel riskid kodukontoris töötamise tõttu. Käesolevas lõputöös analüüsitakse küberteadlikkuse koolitusi ning uuritakse haridusmudeleid ja üksikuid elemente, et toetada küberteadlikkuse videomängude koolitusmeetodit. Videomängude kasutamine õppevahendina ei jää ilma väljakutseteta. Lõputöö uurib nendele väljakutsetele võimalikke lahendusi ja analüüsib eksperimentaalse mängu jaoks ideede kogumiseks mõnda populaarsemat küberkoolituse mängu. Sektretäride fookusgrupile tehakse uuring, et koguda olulist teavet nende IT-kompetentsi, teadlikkuse tõstmise koolituste ja küberturvalisuse usaldusnivoode kohta. Lisaks kasutatakse andmeid eksperimentaalse mängu ülesehituse jaoks. Eksperimentaalne mäng sisaldab põhielemente, nagu süžee, õppe- ja motivatsioonimehaanika, kunstistiil ning stsenaariumid.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 96 leheküljel, 11 peatükki, 13 joonist ja 137 kasutatud allikat.

List of abbreviations and terms

DPI	*Dots per inch*
TUT	Tallinn University of Technology
CSA	Cyber Security Awareness
ICT	Information and Communications Technology
NSAM	National Cyber Security Awareness Month
ECSM	European Cyber Security Month
GFCE	Global Forum on Cyber Expertise
ROI	Return on Investment
ARCS	Attention, Relevance, Confidence and Satisfaction model
DoD	Department of Defense
GBL	Game-Based Learning

Table of contents

List of figures

List of tables

No table of figures entries found.

1 Introduction

"The weakest link in a chain is the strongest because it can break it."
Stanislaw Jerzy Lec [1]

The cyber landscape is expanding daily, as of January 2020 there are according to Statista approximately 4.54 billion active internet users [2], this is met with a demanding infrastructural growth. The digital world is all around us, there is no going outside and not seeing at least a few people looking down on their phones or working on their laptops. The information society is here with all the needs of these online users are met with new online services both home and work life. As cybercriminals don't sleep, there is also a rise in cybercrime, Broadband Search revealed that in the US alone 78 percent of all the organizations has been targeted within the past year [3], and a study from the University of Maryland shows that at least one cyber attack finds place every 39 seconds [4]. Therefore, the overall cyber security awareness needs to be raised – hence being a CEO or not.

Cyber attacks are usually targeting the human part of the security chain, due to crooks seeing it as a weak link. Therefore, in an information society one should be looking at the possibility of transforming this link to the extra line of defense. While cyber awareness is getting more important every day, people keep willingly sharing massive amounts of sensitive data online that could be used in attacks, especially if these people work for targeted companies. Not only high-end employees, like a CFO or a CTO, deal with sensitive company data, average or even part-time employees can also deal with sensitive information and they are many times overlooked, when trying to raise the cyber awareness within a company [5].

Despite all efforts done to raise cyber security awareness, it stays difficult to transfer that concern onto employees. Research about the attitude employees have towards cyber security and risky online behaviors, shows that even though the company policies state not to share any passwords with colleagues and/or click on links in e-mails, they continue to do so. The study also shows that once employees are in their place of employment,

cyber security is no longer their main concern and that depending on the importance of their function within the organization, they either pay more or less attention to cyber security [6]. An article about improving employees' cyber security awareness states that employees still have little concern for the vulnerability their company has to cybercrimes. The ignorance comes from the fact that the employees struggle with the understanding of and compliance with cyber security awareness. That struggle translates directly into the work environment and creates a vulnerable workspace. On top of that, less than half of the employees subjected to the article's questionnaire are aware of their companies' security policies and don't feel like cyber threats pose a real risk. The problem does not just lie with the employees, 51% of the business leaders believe their company is not at risk for cybercriminals [7].

The lack of Cyber Security Awareness (CSA) is a problem, where we, as cyber security communities, need to raise awareness more than ever. "The fact today is that security awareness as conceived is not working" [8, p. 120] The digital world is changing and evolving, it's only logical that cyber security awareness training needs to follow that evolving trend.

Covid19 in 2020 locked down most of the world to a home Office situation for at least two months – some needed to balance both work and educating children in the same situation, while others workload skyrocketed, as they work in the IT sector. Therefore, many needed to change the way they were working – started using social media, sharing documents, videoconferencing and other. In this situation the use of internet services increased due to being unable to wander the shops and streets during the lockdown. People were also pushed into using personal devices – mobile phones, tablets, laptops, PCs that were not always compliant with the company's security regulations. In this study the author will be looking into the situation of the technology being used in a home office environment – what exactly the threats are in the cyber world and why we need to focus on raising awareness in digital safety and cyber security of adults.

Offices usually have cyber security experts to enforce security rules and measures, but the question is what happens in case the office is transported into a home environment. It is important to understand the new challenges that occur when dealing with cyber security in a home office environment, before a proper solution can be presented. The normal transition from an office to a home environment requires many procedures from the

security teams before the transition can be made. Due to covid-19 the shift to home office environments had to be made in a matter of days, giving security teams insufficient time to properly setup security measures, leaving hard- and software poorly configured causing vulnerabilities [9].

A first big challenge at home is that it can be difficult controlling the enforcement of company security policies, even when those security policies are made specially for use in home office environments [9]. Employees are most likely not alone at home, especially during the epidemic, when on conference calls family members or guests might be listening in on confidential information. Nonetheless simple security policies should be in place specifying for example the allowed software that can be used to contact fellow employees or share information [10].

Although a company usually has several desktops for home office employees with all the installed security measures, there are simply not enough computers for a large number of employees. As such, many organizations require employees to use their own personal devices that come with many cyber vulnerabilities [9]. Personal devices most often lack the software needed for secure communication and network channels like a Virtual Private Network (VPN). A VPN protects online activities by encrypting all online connections made from that device [11]. Organizations usually require a VPN to be installed before on-site information and network utilities can be accessed. The employee should always make sure that the VPN is patched to the latest version and has the correct configuration to avoid vulnerabilities in the network traffic. The required communication channels specified by company policies should be used in order to allow secure collaboration, like chatting and video conferencing, between employees. Employees should be made aware of the specific communication channels to avoid (Facebook, VK, WhatsApp), and of the information not to share on certain channels [12].

Personal devices often have multiple e-mail addresses not related to work, which can expose the organization to new vulnerabilities. While business e-mail servers are closely monitored, the personal ones are not. They have weak to non-existent spam filters allowing phishing and other malicious e-mails to easily reach the employees. Phishing e-mails could trick the user into revealing their VPN login details or organization information.

Malware could take control of the VPN software to gain direct access into the organization. Employees should receive additional e-mail security information, policies, and training [12].

Being in a home office environment doesn't change the fact that employees still need to enforce basic cyber security like strong password practices. A report from Verizon Data Breach Investigations revealed that in 2019 alone, 29 percent of breaches involved stolen user credentials. Thus, it is recommended by security advisers that employees use two-factor authentication to add an extra layer of security and prevent hackers from using stolen credentials [13].

Most employees are not used to working from home, thus, being ill-prepared on how to work in such an environment. Working from home can be extra difficult due to all the distractions like childcare, chores and multimedia entertainment. CNBC reports that 32% of employees are distracted mostly by TV, while 27% is distracted by childcare. Productivity expert Laura Vanderkam recommends creating a schedule to maintain focus on the work at hand by implementing a few self-care moments throughout the day. She also encourages avoiding continuous communication with employees by creating some spare moments for checking e-mails and replying to chat messages. Separating home life from work life and communication tasks will boost work focus and leave less room for errors and cyber security vulnerabilities [14].

The second challenge comes from the awareness field itself. It's easy to do training in real life with the lecturer, but there are lots of tests promising the same result – people are aware of regulations and standards on how one should operate (e.g. getting a driver's license). For example, when driving a car, everyone has received proper education on how to drive. But when it comes to using gadgets and surfing on the internet – we are all self-learners with various backgrounds, competences and habits. To change our behavior, one needs to change his/her mind set.

In this thesis the author will try to find a concept for a solution that uses video games as a tool in a home office environment. He will be looking at the challenges that home office provides (gather the data from researches, news, suggested guidelines about security for a home office, as well IT-specialists and security advisors) and will be looking at the serious games in cyber security filed to understand in what genre to propose the solution.

The author will be gathering data from the chosen focus group, adults that are non-IT professionals, and evaluate the concept idea with them using a mixed methodology consisting of surveys and interviews.

Research questions:

1. What are the common cyber security challenges in a home office situation to non-IT professionals?

2. How is cyber awareness commonly delivered to commoners?

3. What gamification and video game scenarios are useful for awareness training in cyber security?

2 Cyber security awareness

This chapter defines cyber security awareness and provides an overview of the current cyber awareness training situation including the missing elements, new methods and approaches.

2.1 Terminology

Before cyber security awareness can be defined, we need to take a closer look at what cyber security stands for, and since cyber security is such a broad and ever-changing term that includes many subjects, the scope needs to be limited.

The term “Cyber Security” lacks a defining lucidity like for example “Computer Security” which can easily lead to misunderstandings of the term, depending on the audience [15]. Sowell quoted; “... a long, time-consuming process of trial and error groping, while creating and refining concepts and definitions to express ideas in clear and unmistakable terms which allow substantive issues to be debated in terms that opposing parties can agree on ...” on the necessity of clarity [16]. While not being a problem in private conversations, this could cause inconveniences at organizational levels and that is why all ambiguity needs to be avoided for the sake of the research. Another inconvenience could be the existence of the two terms “Cybersecurity” and “Cyber Security” having the same meaning, research indicates the disjointed term being more widely accepted, thus it will be the sole term used throughout this paper [15].

Oxford university defines cyber security as; “The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.” [17]. This definition perfectly describes cyber security in the context of the research as it includes the actions needed to be taken by an end-user. Since cyber security can range from a personal scale until a national or even global scale, it should be stated that in this research, the choice goes to personal cyber security, meaning that it revolves around the actions and safety of an end-user and the involved cyber devices.

Now that the meaning of cyber security in the context of the research is clarified, we can properly define cyber security awareness. The InfoSec Institute defines cyber security

awareness as; “a formal process for training and educating employees about IT protection” [18]. The security awareness process can be split up into 3 points [18]:

- Educational programs for employees
- The responsibility that individuals have for company security policies
- Measures taken to check these efforts

The first point revolving around the educational programs has by far the biggest role in the cyber awareness process. It is crucial that employees understand the importance of cyber security and the required security measures. Boyce emphasizes the importance that the employees should fully understand how these security measures contribute to the continuity and growth of the organization [19]. Cyber security awareness programs should in ideal situations try to generate positive behavioral changes and raise the employees’ capabilities instead of just trying to educate [20].

With regards to the previous definition of cyber security and the InfoSec security awareness definition we can define cyber security awareness in the context of the research as the process of training and educating employees on cyber security, on a personal level, regarding the safety of themselves and their cyber devices. This process does not just focus on learning new information, but should also align the importance of security measures and generate positive behavioral changes.

2.2 Situating

The cyber security landscape is built from many domains and sub-domains as can be seen in Figure 1. Cyber security domain mind map as seen by Jiang (Chief Information Security Officer Henry Jiang 2017).

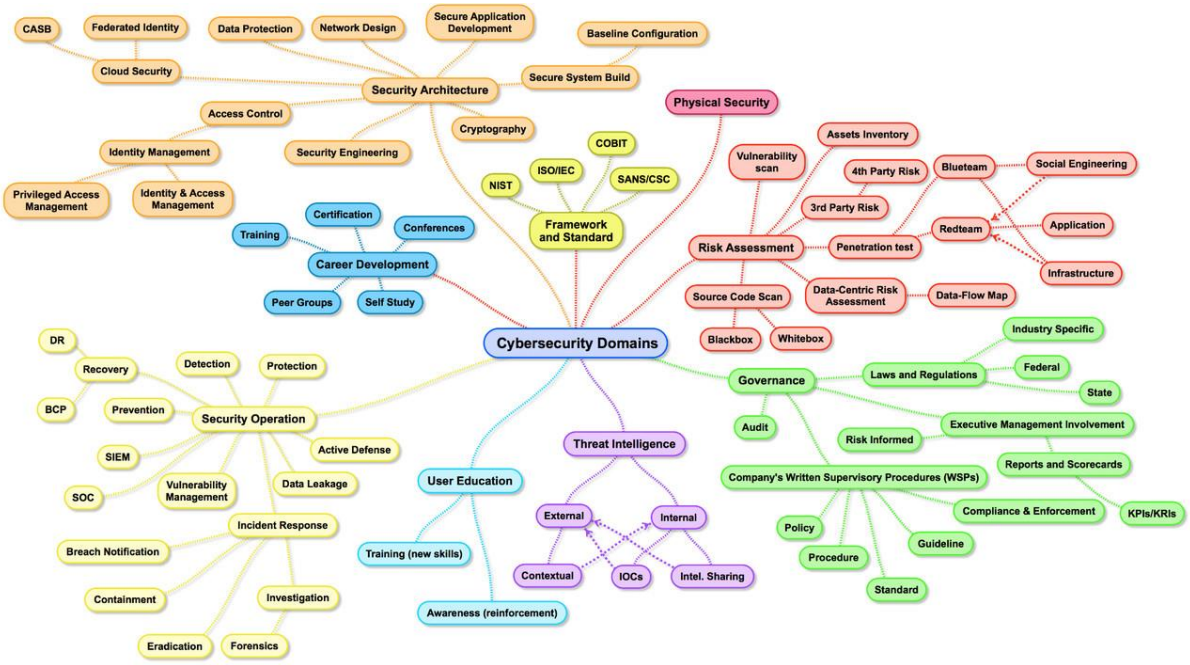


Figure 1. Cyber security domain mind map as seen by Jiang (Chief Information Security Officer Henry Jiang 2017)

The Certified Information Systems Security Professional (CISSP) qualification defines the following 8 domains as of 2018: security and risk management, asset security, security architecture and engineering, communications and network security, identity and access management, security assessment and testing, security operations, and software development security [21].

- Security and risk management: risk management revolves around various analyzing and risk mitigating techniques to make sure that information security objectives are reached. The security model in risk management is to make sure that controls, which should be chosen based on cost, benefit and risk tolerance, are in place to support company goals [22].

- Asset security: assets are material and non-material valuables, considered important to the organization, such as employees, equipment and information. Asset security includes core concepts like data management, longevity and use, data standards, proper retention insurance and data security control determination [23].

- Security engineering: deals with the security and integrity of real-world systems by ensuring those systems meet the envisioned requirements. Security engineering is also responsible for enforcing security policies [24].

- Communications and network security: the scope of this domain is rapidly expanding, as new technologies are being standardized. Communication security deals with creating communication channels that are secure and trustworthy for online conferencing, remote working and online payment. Network security keeps those communication networks and company networks operational and secure [25].

- Identity and access management: identity management revolves around the management of user identities and their privileges, which includes user management tools. Access management deals with the tools and management systems used to limit user access to certain parts of systems and applications [26].

- Security assessment and testing: "the process of analyzing the security standards of a system". Systems and applications are thoroughly inspected and tested for any vulnerabilities, threats and risks. This process includes different steps such as data analysis, vulnerability scans, requirement studies and situation analysis [27].

- Security operations: revolves around the day-to-day access and security of systems, applications and resources. A security operations center (SOC) is usually the division dealing with this domain and the entity making up the required security policies. One of the key points of security operations are administrative controls that include screening of employees and organizing security awareness trainings [28].

- Software development security: creates new secure or controlling non-secure applications following the confidentiality, integrity and reliability (CIA) principles [29].

Having discussed all these cyber security domains there is only one that stands out in relation to this thesis and that is the security operations domain, which is in control of security awareness trainings.

2.3 Awareness training

2.3.1 Effectiveness

There are many studies revolving around the effectiveness and differences of cyber awareness training methods, so in order to evaluate them, it is important to use multiple information sources. CybSafe, a British cyber security company, splits security awareness training into 4 main parts: classroom-based training, visual aids, simulated attacks and, last but not least, computer-based training. Classroom-based training is what most consider as the traditional way of training; the attendees take part in a workshop and listen to an instructor who gives advice and information on one or more security topics. The biggest advantage is that this type of training provides the attendees immediate feedback, allowing the instructor to readjust the learning session. However, this might not be the best way of learning, as adults prefer to learn individually, in addition costs are high and this classroom-based training would have to occur regularly in order for the taught information to stick. Visual aids training uses visual pointers, like posters, to offer limited security advice on important topics such as password management. The biggest benefit of using these aids is that the given information is easy and fast to process. Although easy and fast to process, visual aids are easily ignored and entail no feedback. Finally there are simulated attacks, non-harmful attacks, launched on users to see how they will respond to the threat. The biggest benefit of those attacks is that they can have a powerful lasting phycological impact. There is however a psychological dilemma, some do not morally agree with these simulated attacks and on top of that claim they are unproductive [30].

A study on the effectiveness of cyber awareness methods uses the five-step ladder model to measure information security awareness. They divided training in seven types: educational presentation, e-mail messaging, group discussions, newsletter articles, video games, computer-based training, and posters. Educational presentation includes awareness and behavioral changing campaigns, the sessions are led by a tutor or teacher. Information campaigns deemed effective for raising awareness due to the useful information provided, was found to unsuccessfully changing the audience's behavior and intention for information security. E-mail messaging can be used as a type of remote information providing campaign, the messages contain useful information about various security topics like password management. This method proved effective in raising the recipient's knowledge about those security threats, however there is no control if the

message was fully understood. Group dialogue is a type of awareness intervention method, the group dialogue contains about 15-20 participants where each participant shares their knowledge and experience with the group. The group sessions are interactive and intend to change attitude and social norms. Security newsletters can be handed out monthly or quarterly, although full of useful information and the ability to change attitude towards security awareness there is no control if the employee read it. Posters can be effective while being a simple method and requiring few resources. This method can provide fruitful if combined with at least another one, relying on posters alone is not enough since it cannot explain security concepts. Video games are a great tool to keep engage the player and can be beneficial into changing cyber awareness attitude, however they can rely too much on previously attained knowledge before the game is even started, it can also fail in representing the companies policies. is Computer-based training (CBT); the final type, allows employees to learn at their own pace. This method can be great for gathering new security information although it lacks the capabilities to actively change intentions and behavior [31].

2.3.2 Issues

Although countless efforts being done to raise cyber awareness, research concludes that awareness amongst employees is still low, which brings up the question of what is being wrong with the current training methods. A lot of research is being done on the effectiveness of the current cyber awareness training programs and methods. An awareness training program is crucial for conveying CSA information to the employees, the training program depends on so many factors in order to be successful. A paper that researches on why these training programs fail to change the behavior, states that simply teaching this information, like they would in school, is insufficient. An awareness training program could be more effective depending on whether the information is interesting, actual and simple enough to be followed, and used material not being too general in order for the attendees to be able to relate. Motivation to learn could be stimulated by offering a sort of reward to the participants, or instead of a reward, invoke the participants with a feeling of fear and a way to avoid it [8]. An article studying the pitfalls and issues with awareness trainings from the journal Future Internet, emphasizes a really important problem with the traditional training programs; there is a lack of practical exposure, meaning that the attendees will not picture themselves in the presented situations and the threat will not feel real, meaning that they do not feel obliged to follow the presented

guidelines. Another issue that arises from traditional training, is that it's challenging to portray the misuse of trust used in social engineering attacks [32].

The cyber security company Bromium reveals in a published report from 2017 that larger companies are spending on average more than €260.000 on just phishing awareness training which is an immense amount [33]. The Defence Works, a company focusing on cyber-crime, states that cyber security ventures made a prediction of around 5.5 trillion euro, going to cyber security clean-ups by 2021. Because the costs of CSA training can add up, companies calculate the return on investment (ROI) before deciding whether it is worth investing in an awareness training program, which means that not all companies will spare the expenses needed and remain vulnerable [34].

2.4 Other ways of raising cyber awareness

With cyber awareness training sessions being expensive and showing mediocre results, scientists are looking for new methods to raise CSA. One of these methods studies the use of behavioral science to boost the effectiveness of these training sessions. A report from the Government Office for Science reveals a few extra points-of-view on why training sessions might not be as effective, as initially thought. People are habitual creatures meaning that, even after training, no matter what situation, they tend to fall back on their previous unsafe habits. It seems that risks are downplayed, or simply ignored, by assuming they couldn't possibly be the target of an attack, referring to an earlier mentioned lack of fear. It seems people also tend to over valuate their ability to deal and recognize security threats. The report mentions a few pitfalls to avoid when holding awareness campaigns. It is best advised to avoid click-through information, meaning not just to present the information, but to engage the user more, instead of just having to press the mouse button. The information given to the target audience, should also be tailored, as when too general, the instructed person will not feel related, which is one of the most important requirements to easily retain information [35].

In October 2004, the National Cyber Security Alliance and the U.S. Department of homeland security launched a yearly initiative, called the National Cyber Security Awareness Month (NCSAM), a joint effort between the American government and industry to promote the importance of cyber security [36]. Fast-forward to October 2012, the European Union Agency for Network and Information Security, the European

Commission DG CONNECT and its partners deploy the European Cyber Security Month (ECSM) to raise awareness about cyber security in Europe [37]. A few years later in 2015 the Global Forum on Cyber Expertise (GFCE) is founded, a global platform that offers an exchange of information about cyber practices between private companies and international organizations [38]. That same year, the Global Campaign to Raise Cyber security Awareness Initiative is created, a collaboration between America and Canada. The list of initiatives, organizations and joint efforts to help raise the importance of cyber security is endless, signifying the importance of the topic up to a national and global scale.

2.5 Home office cyber security

ZDNet, a technology news website, reports that the amount of hackers trying to exploit the corona virus outbreak, keeps growing. The growth is directly linked to the increasingly infectious corona virus outbreak. As many organizations set up new networks and VPNs to allow employees to work from home, hackers take advantage of this situation by using publicly known vulnerabilities in VPNs and other remote-working tools [39]. VPNs are an attractive target due to them transmitting sensitive data of shared and public networks and having a lack of layer security in the perimeter defenses, this means hackers have easier and faster access to these networks [40]. Hackers could break the VPN encryption through those vulnerabilities and steal the encryption key or could break the encryption computationally by brute-forcing. A VPN can also leak the original sender's IP which would expose the target [41]. Comparitech reports that in 2018 a malware called VPNFilter compromised approximately 500.000 devices worldwide by infecting routers and network devices [42]. It is thus extremely important to choose a proper VPN tool or configuration using secure settings like AES-256 military encryption and kill switches while avoiding VPNs with known domain name system (DNS) and IP leaks [43].

Corporate devices can be provided to employees working remotely, but a study by Proofpoint reveals these devices are not only used to complete work activities and, on top of that, the study revealed that 55% of the global survey participants extend access to friends and family. Due to convenience and ignorance of the security policies, the users of these corporate devices do not hesitate to login into their personal e-mail or stream music. Besides violating policies, these actions can expose the users to cyber threats by

increasing phishing susceptibility. While corporate e-mail is usually well protected and monitored by infosec professionals, they generally pay less attention to personal webmail and browsing. Proofpoint states that, in order to improve this behavior, employees should be trained to apply cyber security best practices and company policies [44].

Cloud storage is rising in popularity amongst businesses because of the easy usage, versatility, high-storage and cost savings. While cloud storage is easy to implement, there is no control over the data, as the control is fully in the hands of third-party providers. This also means that privacy is at risk when dealing with sensitive data, which could be viewed by unauthorized users. There is also the threat of data leaks, as hackers have already targeted popular cloud service providers or cloud accounts in the past to get access to sensitive data. Some organizations have a bring-your-own-device (BYOD) policy that encourages employees to bring their own devices, which although cheaper, can be dangerous, as compromised devices could access the cloud network from within the company premises [45].

AnubisNetworks, a company specialized in email security services, reports that e-mail is the most frequently used communication channel, making it a perfect target for hackers. In 2018 over 350.000 new e-mail viruses were created to target individual people and companies. In 2017 over 76% of organizations worldwide were involved in a phishing attack. Phishing is a popular method used frequently by hackers in e-mails to trick people and steal their personal data and credentials. Phishing e-mails trick targets by disguising themselves by using official logos of the company and providing a link to a malicious phishing website. Spoofing is another popular tactic, by falsifying the e-mail header, the e-mail looks like it comes from a trustworthy source, a method that is frequently used in combination with e-mail phishing. Malware can also be spread using e-mails; When the target opens the malicious software, its system or network can be compromised and hackers will be able to steal sensitive data. Ransomware, while similar to malware, attacks the target's system and makes it unusable by encrypting various files until the ransom has been payed [46].

Employees working from home often use video messaging apps, like zoom, to contact their fellow employees, which are an essential remote communication channel. Although Security Boulevard states there are only a few security risks, hackers are using this increase in video messaging apps to send malicious e-mails, social network messages and

even text messages containing links of fake invitations to video messaging app meetings. The aim of these malicious messages is to deliver malware and ransomware to steal personal data. It is advised to keep all messaging apps up-to-date and to cover the webcams of work devices, should they have been compromised already [47].

As earlier mentioned in the introduction, employees can be easily distracted at home, 2|SEC, a cyber security consultancy, reports that bored and distracted employees are a big security risk. These kind of employees usually work in repetitive low-entry jobs and spend a lot of their time visiting their favorite websites, social media, even clicking on malicious links on purpose. This kind of behavior can have severe consequences on the companies' cyber security, when left untreated. Cyber security training is part of 2/SEC's recommendations to reduce this issue [48].

2.6 Conclusion

Cyber awareness training has been defined and situated in the context of this research. When researching the effectiveness and issues of various cyber awareness trainings, both the positives and negatives of trainings were discussed, it seems that there is still room for improvement. Organizations and researchers are trying to find new ways to promoted cyber awareness and improve trainings. When looking at cyber security in a home office environment, it seemed there are a multitude of new vulnerabilities the employees are submitted to, which should be considered when working on an awareness training solution to be used at home. The next chapter will discuss the educational possibilities and capabilities of video games to find out, whether a video game solution has the necessary educational capabilities.

3 Educational elements

This chapter takes a deeper look into the educational models and elements a video game could benefit from, to be a viable learning medium for cyber security awareness. It is crucial to establish the correct elements the game needs to maximize the efficiency of the learning process. Every element will be separately discussed and proved by using collected data from related researches.

3.1 Situating

Benjamin Bloom published in 1956 together with collaborators a framework to categorize educational goals called the “Taxonomy of Educational Objectives” also known as “Bloom’s Taxonomy. Bloom’s taxonomy exists of 6 main categories: knowledge, comprehension, application, analysis, synthesis and evaluation. Although each category contains subcategories, the main focus will lie on the main categories. Knowledge is based around the ability to recall methods, processes, patterns, structure or setting from memory. Comprehension revolves around fully understanding or comprehending the discussed materials, without the need of relating it to another topic for better understanding. Application stands for the “use of abstractions in particular and concrete situations”. Analysis involves breaking down communication based on its essential elements, as to make sure the idea hierarchy is clear and expressed ideas made explicit. Synthesis represents the putting together different parts and elements to create a whole. Evaluation refers to “judgments about the value of material and methods for given purposes”. Bloom’s taxonomy can be used for: establishing the learning goals, organizing and clarifying learning objectives and supporting the teaching process [49].

For now, it seems that the apply and understand categories, and later the remember category, are most relevant and related to cyber awareness training due to the practicality of video games. After evaluating the educational models and elements, a more concrete conclusion can be made.

3.2 Educational Models

An Increasingly popular model is Competition-based Learning (CnBL), which is used to boost the motivation and learning performance of students. CnBL is a methodology that uses competitive elements to achieve a positive learning experience. Competitive elements include mechanisms, like a score or level tracking system, so that participants can compare themselves to others. CnBL is highly flexible, causing it to be frequently combined with other methodologies like Case-Based Learning (CBL), Problem-Based Learning (PBL) and Project-Based Learning (PjBL) to optimize the learning process [50].

Case-Based Learning is defined by Yale as "an established approach used across disciplines where students apply their knowledge to real-world scenarios, promoting higher levels of cognition". A case consists of multiple realistic scenarios, with one or more characters, to support the story in those scenarios. CBL develops the students' extrinsic and intrinsic to learn, while also highlighting self-reflection and critical reflection. When using CBL, it is crucial having a powerful story, versatility and a streamlined self-guided learning process. CBL is often combined with Problem-Based Learning. On top of that CBL has already been successfully implemented in medical, law, and business schools, and undergraduate education [51].

Problem-Based Learning relies on the use of triggers from a problem case originating from a complex real-world scenario to promote the understanding of concepts and principles, as opposed to all the facts and concepts directly presented to the learner. PBL stimulates the development of skills and abilities like, critical thinking, problem-solving and communication skills. Group teaching can also benefit from PBL by researching and evaluating research materials and can even provide life-long learning. PBL is extremely versatile, meaning it can be implemented into a wide array of learning situations. Strictly PBL is used for the entire duration of the semester as the primary method of teaching, when integrated in a curriculum. However, this is not exclusive, PBL can be used in labs and design classes, or even to start a discussion. The real-world problem is the thread connecting these various usages. Although PBL can be a useful strategy, it is compared to CBL, an open sort of inquiry, while CBL is a guided process that makes more sense in the cyber awareness training industry [52].

Project-Based Learning is “an instructional methodology that encourages the student to learn and apply knowledge and skills through an engaging experience”. PjBL allows students to deeper learn in-context and to develop various common skills. A project is always related to a real-world problem just like Problem-Based Learning. Projects require the student to engage in a process of learning, solution building and product construction, in order to solve a real-world issue or challenge. PjBL can be used to see how students apply academic content in different new contexts and in real world applications. Students are more independent from their teachers, as the role of the teacher is to be a facilitator or project manager. Therefore, students are stimulated to make their own decisions on how to do their work best, which will demonstrate their understanding of various studying materials [53].

The ARCS motivation model is developed by John Keller and focusses on motivation. The model is entirely based around the continuity of the learner’s motivation during the educational process. The ARCS model consists of 4 components, Attention, Relevance, Confidence and Satisfaction. The Attention component focusses on maintaining the learner’s attention span and interests. The usefulness of the content should be portrayed in the learning process to satisfy the Relevance component and help learners bridge the gap between real-world and content. The Confidence component focusses on expectation development; keeping the expectations of the learners realistic and positive is important to the success expectation on the learning process. Motivation and satisfaction are directly related to each other; learners should have a feeling of satisfaction when proceeding through the learning process [54] [55].

3.3 Educational elements in video games

Now that some general educational models have been discussed, it is time to take a closer look at what individual educational elements a video game could benefit from, when trying to raise cyber awareness. The elements were found after analyzing cyber awareness in chapter 2 “cyber security awareness” and will be analyzed and discussed, when such elements are achievable inside a video game of course.Cyber security awareness

3.3.1 Relatability

The term “Relatable” means the possibility to understand, like or have sympathy for, because of similarities to oneself or one's own experiences [56]. This feeling can be

achieved by creating meaningful stories, giving a relatable experience to the user [57]. A real-life application is an application that is drawn from actual events or situations [58]. The relatability factor can be introduced into a real-life application by wrapping the game's activities into a story preferably with visuals. It is also crucial to take into account the social context meaning [57]. An idea can be clear to one group of people, but confusing to another group, that is why it is important to consider the social context. Alaa states that meaningful communities, also known as the 'people factor', combined with relatedness, should further improve the experience for the user. He also states that fun can originate from social interactions, further enhancing that experience. It is also of utter importance that the social interactions make sense on the game design level and also to the narrative, if there is one of course [59].

Groh summarizes the principle of relatedness as [57]:

- The connection to personal goals
- The connection to a meaningful community of interest
- Meaningful story
- Consider the social context meanings

3.3.2 Rewarding

The term "Rewarding" stands for something that gives you a feeling of satisfaction and pleasure [60]. An experience that is rewarding, alludes to an activity that is done without the expectation of a future benefit, but instead, because the experience itself, is fun and interesting. Educational games are no different, if the flow of the game is made out of learning elements, in which the player is willing to partake, without the expectation of a reward at the end, only then the game supports an ideology of life-long learning [61]. A research about the enjoyment of video games states that rewards should benefit from the way a player learns to play a game and that the reward should equal the performance and time invested in the game [62].

A study about the effects of gamification compares the gamification effects on an educational course site. One course page was gamified meaning that it had a leaderboard, badges and levels, while the other course page remained unaffected by these elements.

Before the test even started, the gamified site had a significant difference in view rates showing more motivation from the students. While almost all of the students with access to the gamified site posted on the forum, 70% of the students with access to the non-gamified site did not, showing a clear lack of motivation. The study concludes that the students from the gamified course site were stimulated to spend more effort on learning [63].

Based on a variety of surveys and video game analyses Wang and Sun propose the eight most common reward forms [64]:

- Score system: the usage of numbers to indicate a player's performance, which has no direct impact on gameplay, but will be used by players to compare themselves to others.

- Experience system: experience points can be gained by executing game tasks and achieving specific goals. Experience points can be used to unlock items or upgrade the character.

- Item system: in-game items that grand special abilities or alter the appearance of the player.

- Resource system: valuables that can be collected and used as a form of currency or a way to obtain in-game items.

- Achievements: special titles that indicate the effort the player took, in order to achieve a certain goal.

- Feedback messages: a form of direct indication of the successful completion of a task.

- Visuals: pictures or video clips that follow important game events, also used for supporting the narrative.

- Unlocking mechanism: the unlocking of new game content, once specific requirements are met.

3.3.3 Practical experience

The term “Practical” stands for the involvement or concernment with experience or actual use, not theoretical [65]. Active learning is a process in which the person interacts or participates with the educational activity [66]. Games require a player to participate and make decisions in all parts of the educational process and they also allow the player to practice real-life situations in a realistic environment and encourage reflection about his/her skills. Simulations are a sort of simplified reality with the goal to have a player interact with a simulated reality. It is important that the created virtual environment contains essential elements from the real world [67]. The term “Video Game” itself stands for an interactive activity, in which a player engages in [68]. Thus, we can conclude that games naturally provide a hands-on experience.

3.3.4 Realism

The term “Realistic” stands for the representation of things in a way that is accurate and true to life [69]. Realistic video games are hard to define; even when video games contain unrealistic elements, they can be perceived as realistic, when relative to a reference point, even when that element does not exist in real life. Realistic video games are often only partially realistic, since real life does not contain all elements that a game environment could have [70]. Wages states that the realism of a video game world and non-player characters can be split up into perceptual realism and social realism [70]. Perceptual realism, on the one hand, also known as naïve realism, represents our perception of objects, how they really are [71]. Social realism, on the other hand, represents our perspective on social and political attitudes [72]. Wages also states that the stimuli triggering human senses, can be split into essential and non-essential information. Most of the information that creates the real world, is non-essential and will therefore be ignored by the brain when creating an image of the real world [70]. Masahiro Mori was a robotics professor that came up with the ‘Uncanny Valley’ principle. This principle states that a real human’s reaction to a humanoid robot, which is not perfectly modelled, will be a repulsive one, even scary. However, if the robot is clearly a robot, or is a perfectly modelled one, the eerie reaction disappears [73]. A visual representation of the ‘Uncanny Valley’ can be found in Appendix 1 – ‘Uncanny Valley’ Principle. This principle can be applied to the virtual environment, the game environment should be either perfectly modelled to the real world or purposely in a less real-world style [70].

Simulation games are not just good for hands-on experience, but, as the term suggests, for simulating realistic activities from the real world. A research about the development of active learning with simulations and games states that the development of a simulation game is foregone by the following steps [67]:

- Define a clear goal: the purpose must be clear; when there are too many different activities required to complete a goal, it becomes unworkable.

- The use of randomness and stress: randomness is a good simulation of the real world and stress can be beneficiary to the learning process.

- Create the environment: it is important that the game environment has a relation to the goal and setting of the game; a complementary environment can benefit the learning goals.

- Create a clear role for the player: in the real world everyone has a specific role in each environment; the game environment should assign a clear role to the player, so that it's clear what must be done.

- Create an evaluation type: in simulations are no typical winners or losers; it's about the process, which can have a good or bad evaluation. It is crucial for goals to be measurable, so that they can indicate the player's progression and understanding.

3.3.5 New habits

The term "Habit" stands for the usual manner of behavior acquired by a frequent repetition of or exposure to that behavior [74]. A research taking a deeper look at healthy habit forming through the use of a mobile phone, defines 7 states in the healthy habit-forming process. Users first start in the "Intention" state, representing people who are willing to make a change. This state represents all of the people with bad cyber security habits. Once the learning process starts, the users move to the state "Planning", planning can be seen as the combination of 3 other states; "Initiative", "Maintenance" and "Recovery". Recovery can result in trying again and moving back to the state "Initiative" or in "Quit". The "Maintenance" state is the most important one and relevant to our study, while also being the only state that can result in "Success" [75]. Wohn states in a study

about habit strength in social network games, that repetitive tasks, like forcing the user to click multiple times, make a significant contribution to the habit strength [76].

There are already a bunch of habits improving games out there, like “Zombies, Run!”, a game that stimulates running by linking the running activity to running away from zombies, or EpicWin, a game that uses gamification to encourage the completion of to-do lists [77]. Zenn, an employee at GameAnalics, narrows down on some of the points required, when building a habbit-forming game. Firstly, it’s important to make the game responsive and well-paced, as letting players wait unnecessarily, is a no-go, and the players should feel like they have accomplished something to stay engaged and feel productive, key steps into creating habits. Secondly, it is important to keep the player interested in the game by making sure that there is always something to do, even after completing a certain goal to keep the player involved [78].

3.3.6 Improved learning

There are many studies available about the educative qualities of video games, but one thing they all have in common, is the importance of the cohesion between the learning objectives and the gameplay. When the learning objectives are separated from the gameplay, the educationally effectiveness will be reduced. A research about the design principles for flow experience in educational games states that the goal is to strive for an “Optimal Experience”, a state in which the player is so involved with the activity, that he wants to do it purely for himself and his enjoyment. In this optimal experience the player is more receptible to retaining educational information. The game flow is the main factor, when trying to achieve such an experience. In the description of the flow antecedents is stated that it is important to provide immediate feedback to the player, when he fails or completes a goal or action and that the result of that action should be a short process. The more a player is focused on the game activity and forgets all unpleasant thoughts, the better for the game flow. Game goals should be spitted up into smaller more achievable sub-goals, which should be introduced at an appropriate pace to keep a level of success for the player [61]. De-Marcos concludes from his experiment that, when games make use of extrinsic motivators like a competition between the players, the learning performance is boosted. When comparing results between one educational game and another that integrates social aspects, the results reveal that the game with social aspects, shows more promising educational results [79]. Fisch recommends in his study on making

educational games “Educational”, to use some sort of hint and feedback system, so that when failing a task, the player is able to learn from his mistakes. It is important that the feedback does not present a direct answer to the problem in order to keep the user trying to figure out a solution. Feedback messages should not be generalized like “Sorry – try again”, as that will hinder the learning process [80]. A paper on engaging in e-learning states that gamification helps raising the stimulation students need towards learning. The positive feedback they get during gameplay has a big role in this process. It is stated that, because of the gamified experience, they will be more motived to study at home, showing promising lasting effects [81].

3.3.7 Elements Summary

The researched game elements are neatly summarized in this chapter. According to the research these elements all support an efficient cyber awareness game learning experience. What follows now, is a short summary per element:

1. Educational: This element relates to the efficiency of learning through video games discussed in Section 3.3.6. It is most definitely possible to build a game that can be used for learning, but certain game elements are required besides providing the player with just information in order to make them learn and remember.

2. Relatable: It is important for the player to feel relatable to the game as discussed in Section 3.3.1. When the player is feeling disconnected, this will work against the learning process. Making a relatable game is possible to target specific audiences, if certain game elements are included to make the experience feel more personal.

3. Practical: The practical element is closely connected to the realistic one in order to be able to provide a learnable hands-on experience as discussed in Section 3.3.3.

4. Realistic: Based on the connection to reality and practicality the best game type suitable for this experience is a simulation game. We also discussed in Section 3.3.4 that a game does not have to perfectly reflect reality in order to feel like a realistic game.

5. Habit-forming: It is important that the learned cyber awareness behavior becomes a positive habit in the daily lives of the players. In Section 3.3.5 we found out that it is certainly possible by the use of certain game elements to induce new habits.

6. Rewarding: In Section 3.3.2 we discussed the use of intrinsic and extrinsic motivators to reward players for playing the game and completing game objectives. We also discussed possible ways to implement those reward features.

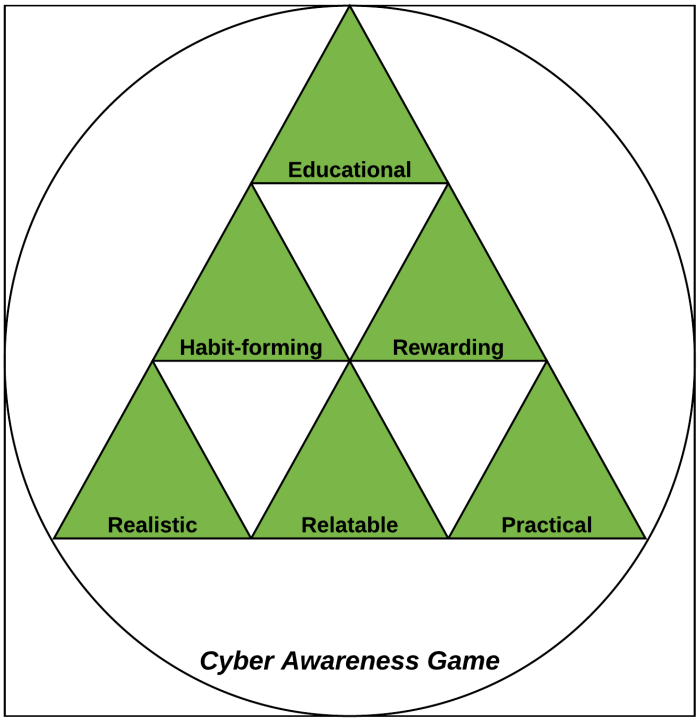


Figure 2. Cyber awareness game elements

3.4 Conclusion

Cyber awareness sessions are a guided process, thus, it is only logical that the game should provide a guided learning experience as well, the educational model that revolves around a guided learning experience is case-based learning. As explained, case-based learning is mostly used in combination with another educational model to extend the educational benefits. The ARCS motivational model on the other hand has very close ties to most of the researched educational elements, while also fitting in perfectly with case-based learning due to their theories, having no conflicts. A pilot game could be structured using both the ARCS motivational model and case-based learning.

After separately evaluating the educational elements it is clear why and how they can be achieved in a video game. Referring to Bloom's taxonomy the case-based learning model fits perfectly into the apply and understand category. The next chapter is going to discuss what games are, their challenges, and some example games used in education already.

4 Games

This chapter takes a closer look at serious games, educational games and gamification, and their respective definitions. It will also provide an overview of game characteristics and discuss the results of game implementation in education. Furthermore, there will be a listing and discussion of already existing cyber security and cyber security awareness games.

In 2013 the Estonian government turned to the use of video games for educational purposes, by financing a game called Uos, which was supposed to teach children on how to use the e-government system. However, due to poor execution, the population of Estonia considers this game to be a joke [82], so that's why it is important to analyze games, their characteristics and elements in order to determine the best combination of elements for an educational game.

On a more serious note, games are already actively used in a wide area of fields. For decades educators have been using games to stimulate learning and are already reaping the rewards [83]. Games like simulations already play a big role in the military, schools and industry to teach certain educational materials [84]. In the military, commercial games are being used for the measurement of the eye-hand coordination, while simulations find themselves used by pilots and tank operators to prepare themselves in real-case scenarios without having to take any actual risk [85].

Another example, showing the popularity of video games finding their way into the educational system, is an economics focused game called Miniconomy. Miniconomy is a popular browser-based game used in some Belgian schools. The game engages groups of economy class students to compete against each other and strive to have the most successful business, while also learning and mastering the basics of starting a new business in a fun and interactive way. The top 3 students with the highest revenue businesses often get a reward from teachers to motivate students to play the seriously [86].

4.1 Defining games

Millennials are the first generation to grow up with extensive and easy access to video games. According to a report on the gaming habits of millennials, the majority continues playing even while having families and full-time jobs [87]. This shows that the new generation workforce would benefit even more from education through video games, since they are so accustomed with them. The video game market segment keeps growing, supporting the idea that video games get an increasingly bigger role in society. A report on certain game studios, hitting sales records during the corona epidemic, shows that people turned to video games during the lockdown [88].

Games are continually being redefined and there seems no agreement between the defining parties about the definitions. It is thus of utter importance that the term “Game” has a proper definition in the context of the research before the term “Video Game” can be defined. Oxford defines a game as “an activity or a sport with rules in which individuals or teams compete against each other” [89], Webster states that a game is “a physical or mental competition conducted according to rules with the participants in direct opposition to each other” or an “activity engaged in for diversion or amusement” [90]. Arjoranta suggests using a Wittgensteinian approach when validating game definitions instead of the common core approach to properly create a redefinition that wouldn’t per se completely exclude certain game definitions [91]. Although for simply defining the term “Game” in the context of the research, it is deemed unnecessary due to the fact that the focus lies on the term “Video Game”. As such, based on the Oxford and Webster definitions, the term “Game” can be defined as an activity or competition in which the player competes against other players or for the entertainment of himself.

Games can be split into three main categories: tabletop games, party games and video games. Tabletop games are the oldest category out of the three; a game called Senet has been dated back as early as 3500 BCE. Tabletop gaming is a term used for games that need to be played on a surface or table, the game usually makes use of game pieces or other accessories like dice and cards [92]. The second category of games, party games, are games meant to be played at social gatherings to stimulate interaction between the participants and provide a form of recreation for a group of people [93], some popular party games are “Never have I ever” and “Truth or dare”. The third and final category, video games, has diverse definitions. Video games are defined by Merriam-Webster as

“an electronic game in which players control images on a video screen”. Whenever the term “game” is used within the thesis to raise cyber awareness that term always refers to video games unless specified, not tabletop, nor party games.

The term “Video Game” has just like the term “Game” no consistent definition due to the fact that there exist so many different instances. Although containing the word “Game”, video games should not be taken lightly, James Newman States; “While scholars identify a range of social, cultural, economic, political and technological factors that suggest the need for a (re)consideration of videogames by students of media, culture and technology, here, it is useful to briefly examine just three reasons why videogames demand to be treated seriously: the size of the videogames industry; the popularity of videogames; videogames as an example of human-computer interaction.” [94], implying the need for a proper definition in the context of this research. Keeping in mind with what Newman stated, Esposito formulates a fitting definition for what a video game is; “A videogame is a game which we play thanks to an audio-visual apparatus and which can be based on a story.” [95]. The audio-visual apparatus in this definition stands for any electronic system that contains computing abilities, accepts input from a user and outputs audio and video [95]. The definition Esposito provides is versatile enough to fit in the context of this research and thus will be used.

4.1.1 Video game genres

Video games can be divided in different genres depending on a number of factors. A genre could be defined by the setting or story, but is most of the time defined by the kind of interaction, the user has with the game [96]. It is important that the most common top-level genres are properly explained to provide a better understanding of the possible types of video games. Matthews lists and explains 8 main genres [97]:

- Action: The action genre is defined by giving the player full control of the action, while putting the player in the center of it all. The action itself is composed of multiple physical challenges that must be overcome by the player. Action games tend to be relatively easy to allow any players to be able to play the game, which is part of the reason that they are so popular. A prime example of an action game is the subgenre “Shooter” in which the goal is to take out the opposition by shooting weapons [97].

- Adventure: The adventure genre is defined by the interactions that players have with the environment and other elements in order to solve puzzles and be able to progress the story or gameplay. Because the story progression is the main goal and there are usually not much traditional action game elements, the genre finds itself to be less popular amongst gamers. Adventure games were originally text-based, offering the player text-commands to execute in-game actions [97].

- Role-playing: The role-playing genre is defined by the player being able to build his character and the ability to influence the story by the choices he makes. This means that role-playing games usually have different alternative endings. The subgenre MMORPGs (Massive multiplayer online role-playing games) allow hundreds of players to interact with each other in an open world and is amongst the most popular game genres [97].

- Simulation: The simulation genre is defined by the emulation of real situations and events. This allows the player to execute real-life like actions in a virtual environment. The genre includes many possibilities, like construction and management simulations, which allows the player to construct and manage his own city or project. There are also many educational possibilities as discussed before by the military example [97].

- Strategy: The strategy genre is heavily based on the traditional strategy board games giving players most, if not complete, access to the world and its resources. The genre requires players to use, as the name implies, strategies and tactics to pass challenges. Depending on the type of game it can be played either turn-based or real-time. An all-time classic is the tower defense subgenre where players fight off enemy waves to survive as long as possible or to destroy the enemy base [97].

- Sports: The sports genre is just like the name says a genre that simulates real life sports like football, basketball, golf and others. In these types of games the player usually competes against an ai-controlled opponent or real life player. A widely popular subgenre is racing, players have to race against opponents to try and get the best finish time possible [97].

- Puzzle: The puzzle genre is defined by the player having to solve a problem before being able to advance the action, by which the problem is usually displayed on a single screen. A classic subgenre is the logic game genre, of which a popular game is Tetris, wherein a player needs to rearrange blocks to form lines and receive points [97].

- Idle gaming: The idle gaming genre is a relatively new genre that requires minimal involvement from the player, usually by clicking on an icon repeatedly. Players are rewarded upon achieving certain goals and objectives. A very popular game in this genre is Cookie Clicker, a game in which the player has to click a cookie in order to gain points, which can then be used to buy upgrades to speed up the process [97].

4.2 Gamification

The rise of digital game media in entertainment has been anything but stagnant for the past 15 years. The success is visible through the record-breaking amount of console sales and online game environments filled up with players. While video games are a relatively new technology, nondigital games date back far throughout the ages as a common tool used for entertainment; thus, gaming has always had a big impact on society. Once gaming was widely available on digital media and gained it's incredible popularity, research began for its adoption beyond entertainment [98].

The umbrella term "Gamification" is a term used to indicate the use of video game elements in non-gaming environments and systems. Gamification is often used to increase the users' motivation, engagement and overall experience. There have been many studies on the effects of gamification and how to best achieve them. Studies tend to look at the impact of game aspects to reshape behavioral patterns and to the aspects that can be used to recreate an enjoying experience in formal tasks. Economic and social studies take a look at the bigger picture, in their respective contexts, on how to benefit from gamification [99].

Gamification already knows successful implementations in various environments like in the US army. The US army developed their own military shooter game as propaganda to get players interested in joining the army. The world of sports also found a suitable place for gamification, various fitness training apps introduce video game elements like badges and achievements to keep the users motivated in following their schedules. Another example that Starbucks has implemented is the "My Starbuck Rewards" program, by which customers can increase their loyalty level linked to the number of purchased goods. Increasing their loyalty level rewards users with coupons for discounts and free products. A final example of a gamification product is Project Wars, a motivational tool to stimulate people into finishing their projects. It works by displaying a progress bar to reflect the progress of the project by splitting it up in measurable tasks [100].

4.3 Serious and educational games

It can be very easy to confuse serious and educational games with each other, that's why it is so important to define both and indicate their differences. The term "Serious Game" is applicable to a wide range of application areas including military, education, government and healthcare. Since serious games cover so many areas, it is no surprise that there are lots of discussions about the exact meaning of the term, meaning there are plenty of definitions available to choose from. It is determined by using the common core approach that serious games are games that are used for other purposes than just for entertainment. There are a lot of overlapping areas in serious gaming like edutainment, e-learning and (digital) game-based learning, which can make the positive effects of such games questionable. Although having its clear advantages, it is not so that every game automatically benefits all learning outcomes [101].

The Serious Games Initiative was launched to promote the use of games to engage the public: "The Serious Games Initiative is focused on uses for games in exploring management and leadership challenges facing the public sector. Part of its overall charter is to help forge productive links between the electronic game industry and projects, involving the use of games in education, training, health, and public policy". Further supporting and building upon this definition are Susi, Johannesson and Backlund with a definition of their own: "The application of gaming technology, process and design to the solution of problems faced by businesses and other organizations. Serious games promote

the transfer and cross fertilization of game development knowledge and techniques in traditionally non-game markets such as training, product design, sales, marketing, etc.", this definition perfectly describes serious games in a wide range of contexts and, as such, is the preferred definition in the context of this research [101].

When referring to "Educational Games", it is pointing to one of the many areas that serious games cover. While not the same, some consider educational and serious games to be more or less similar [101]. Ge and Ifenhaler define educational games as: "games intentionally designed for the purpose of education or those entertainment games that have incidental or educational values. Educational games are designed to help people understand concepts, learn domain knowledge and develop problem solving skills as they play games" [102]. While it can be seen with this definition, why some consider educational and serious games to be the same, it is obvious that it directly relates to just an area of the serious games concept. This is further illustrated with Figure 3. Comparison model between games, serious games, and educational games.

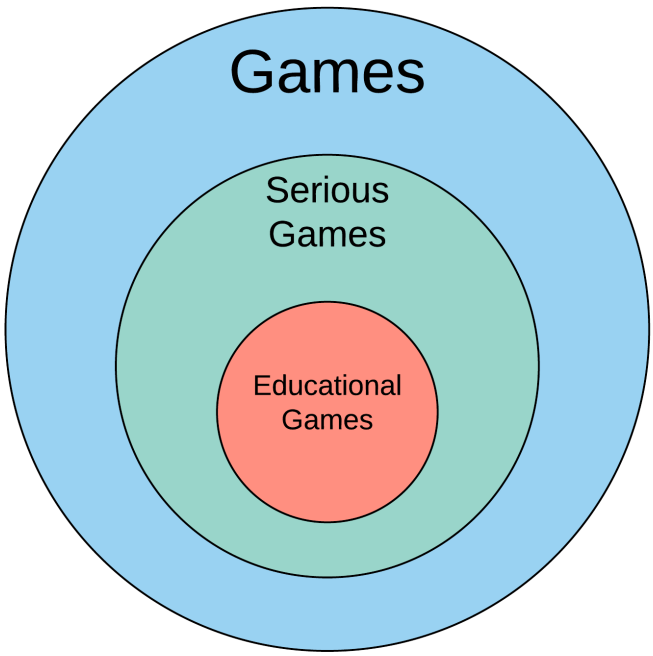


Figure 3. Comparison model between games, serious games, and educational games

4.4 Challenges

There are several challenges when using games as a learning medium. This chapter will look at the most prominent ones and explain which ones can be solved, and which ones can't.

4.4.1 Framing-related

Actually not every person is digitally native as stated by Whitton; individuals can have variances on aptitude, attitude and access to technology [103]. Usually games require the understanding of existing conventions to support their play, which can be troublesome for people who never played games before (e.g. interaction interface) [104]. Additionally not every person likes games or has any interests in playing one; an unwilling player can even disrupt the game for the other participants [103]. Even a subset of the group of people who like to play games is a problem group, as the highly competitive players may miss the learning goals entirely by only focusing on getting the highest possible score. Competitive framing may also promote cheating, as the player could be solely focussed on getting the highest score, which does not mean the player learned anything when the highest score is achieved by abusing an in-game mechanic. Unreal gameplay consequences can break gameplay immersion and ties into the issue of games not being real, there should be some form of bad consequence punishment (e.g. performance assessment or social feedback) [105].

4.4.2 Learning goals

People have different learning styles, as such, an educational game experience will not benefit everyone. Although the average person may enjoy learning more and weaker learners might do better, it is possible that this might not be the case for the more talented people of that educational subject [106]. Whitton [103] and Lainema [105] state that without proper reflection after the game has been played, faulty and unreliable results might be produced. Kim states that without a debriefing, even when the intended information was learned, the acquired knowledge will likely fade away [107]. The educational content is optimally iterative, so that more challenging tasks rely on previously acquired information and add more learning content gradually [108]. It can be challenging to decide the level of difficulty, the level should neither be too easy, nor be too difficult to match player skills accordingly [109]. It is important that a game activity

or task does not become too much or too little fun, so that a player can be to much engaged in the play and procedural content is applied without the proper reflection, losing the learning goals [109]. However, if an activity becomes stale and boring, the iterative content will again not be reflected upon failing the learning objectives [108].

4.4.3 Assessment

As using performance measurement as the key factor in deciding the amount of learned and acquired knowledge, is not always correct, the player with the highest score might not be the person who learned the most, on the contrary, it could be the player with the lowest score instead [105]. Some players could play intentionally bad to experience and learn from the consequences of bad decisions, which is called “functional bad play” and would not work well in a performance-based evaluation [110]. More complex games can have a damaging effect on the learning capabilities; the more different learning elements there are present in the game, the less a player can be trusted to retain that knowledge in a single sitting [111]. Games deployed in an educational context reflect not just the curriculum needs because of the subject matter, not being neutrally treated. The game designers unintentionally embed their own values into the subject material when designing ways to represent that material within the game environment [108]. The player’s experience of the game should be taken into account; when making an assessment, it is important to review how they perceived the challenges [105].

4.4.4 Costs

Creating a video game creates many costs, depending on many factors, due to the complexity it takes to develop a game. The first big cost is the salary for a development team; a development team needs to fulfil many different functionalities and grows exponentially depending on the size of the project. A development team can consist of, but is not limited to, game designers, programmers on the game customer side, graphics and animation engineers and sound designers. The second big cost, a critical part of the development cycle, is testing: the game needs to be tested regularly on its functionality, regression, security and performance. Thirdly come all the costs for the various development software: software licenses and intellectual property, like rights, to a certain brand or character. Developers need expensive equipment; since games need powerful computers to be compiled and ran on, the costs just keep growing and growing [112].

4.4.5 Hardware

A game may not always be playable on a computer, the components a computer is made of (e.g. hardware) determine whether a game will run smoothly or not. The more powerful the components are, the better the game will function. Games on older or weaker computers will run slower or will not run at all. The most important components for video games are the central processing unity (CPU), the video card, ram and storage. The required hardware specifications depend on the game itself [113].

4.4.6 Solvability Challenges

Just as there is a segment of people that do not like traditional learning, there is always a segment that is going to dislike learning using video games as a medium, although that segment, as shown by Hamari, Koivisto and Sarsa, is generally smaller [114]. Although identifying the learning tasks and goals can be difficult in order to frame the educational content and the difficulty of the in-game challenge related to that content, surveys can help with that by allowing the target audience to indicate knowledge gaps and discussion topics [111]. To prevent acquired knowledge from fading away upon finishing the game, the content is best made iterative to make it more rememberable [108]. The game could be split up over multiple days, as to let the content be refreshed over time and stimulate retainability [107]. In order to be able to do a proper assessment of the player after he finished playing the game, his experience should be taken into the play and points could be scaled, based on the performance on the first few tasks, in order to properly measure how much growth there was at the end [105]. The total cost is likely the most difficult challenge to deal with, as costs can be lowered considerably by using open source software and free libraries for the game's content. But in order to create a proper learning experience, heavy costs will have to be made [112]. Hardware is always going to be an issue, but a game can be optimized by decreasing the hardware requirements [113].

4.5 Cybergames

There is already a wide range of multi-purpose cybergames available today, some of which are more technically focused, while others care more for the human side of cyber security, e.g. the cyber awareness aspect. This chapter will look at some of the most researched and used games in the field in order to find out their focus areas and whether security of home office environments is included. The analyzed games are limited to educational cyber security and awareness games.

4.5.1 CyberCIEGE

CyberCIEGE is without any doubt the most popular cyber security game, occupying many of the first given results, when searching online for a cyber security game. The development of the game has been sponsored by the US Navy, the Naval Education and Training Command, the Office of Naval Research, the Biometrics Task Force, the Office of the Secretary of Defense and the National Science Foundation [115].

The goal of CyberSIEGE is to aide a computer security education by creating a simulation consisting of construction and recourse management. The player is the decision maker in an enterprise ranging anywhere from a small business up until the military. The game provides over twenty preprogramed scenarios covering different security topics that include a series of choices for the player to choose from. Each choice can have a significant impact on the security of multiple company assets. The decision process finds place inside a virtual three-dimensional environment representing an office. The office is populated by non-player characters that need access to those company assets in order to progress the scenario. The player is tasked with purchasing new assets like workstations or securing permissions in order to satisfy the needs of the non-player characters. During these processes it is important that the player keeps track of the in-game economy to be able to finance the enterprise. Assets can also be attacked during the scenario with viruses and other dangers, thus, it is important that the player can identify asset related vulnerabilities and mitigate incidents by using and configuring various in-game protection mechanisms [116].

Security scenarios included in the game can be configured by a special tool that is shipped with the game itself. Organizers can, using this tool, customize already existing scenarios and create totally new ones, fitting their educational programs' objectives. The game also

includes a sort of encyclopedia containing proper explanations of all the security concepts that are included in CyberCIEGE. All the standard scenarios include a lab instruction manual for the students to follow and to guide the teachers. Students need access to a computer running the windows operation system in order to be able to play the game [116].

CyberSIEGE brings context to various computer security related concepts by the creation of a virtual learning environment where, by the use of an interactive and visual virtual word, the student can narrow the gap between the terminology and abstract functions. This allows students to better understand how security policies could be implemented using a series of protection mechanisms, physical security and policies. The game allows the player to find the best suited solution by giving the player the tools to experiment without presenting the "best" solution on a silver platter, this enhances active learning through trial and error. The game also promotes active thinking by requiring the students to apply learned concepts from one context into another one [116].

Although CyberSIEGE has promising results and feedback after years of being utilized in schools and other organizations, the basic information assurance awareness has not been fully assessed yet [117]. Through the creation of new scenarios, a home office environment could be set up [116], but since CyberSIEGE is more of a strategic game focussing on IT security students, the educational goals point towards the more low-level technical configuration to mitigate and prevent attacks excluding non-IT professionals. CyberSIEGE is an impressive educational game, suited in specific educational environments, perfectly capable of raising cyber awareness, but is purely for the use of non-IT professionals; as described in the context of this research it remains unsatisfactory because of its too low-level.

4.5.2 CyberAware

CyberAware is a mobile app developed to target cyber security education and awareness, including topics such as firewalls, antivirus software and e-mail spam filters. The app wants to offer an alternative and entertaining educational experience to help learners raise their knowledge on data security issues and awareness. In the app the player is opted to make a choice from a list of security topics and each topic consists of a series of mini games centered around that topic. When the player completes a mini game, the part of a shield is added, upon completion of all the challenges the shield is unlocked granting the

player a final challenge, rewarding the player with a “CyberAware certificate” on completion [118].

The app follows the Attention, Relevance, Confidence and Satisfaction (ARCS) motivation model. ARCS is a combination of various motivational models unified in the context of social learning theory, the model represents a design process to promote the motivation of the learner during the learning process. The key factor in the app is the use of motivational boosters and maintainers, to keep the learner engaged in the educational process; the educational results point to a higher success factor, the more the learner is motivated. One of the key components in the ARCS model is relevance, which is accomplished by the storyline and its relation to the mini games. To boost the confidence of the learner, the learning material is specially designed with realistic expectations and clarity. The mini games also offer an increasing difficulty, when the player progresses to keep the players attention and interest [118].

By the use of questionnaires CyberAware was able to determine the effectiveness of the game on students, before the game was played, 32.6% of all students was able to correctly identify the 4 internet-connected technologies. This number was raised by 15%, after the students played the game and retook the questionnaire. Showing a similar trend is the recognition of the scenes where an internet connected device needed to be protected; before playing the app, the amount was 18.6%, after playing the game, it was almost doubled 32.6% [118]. The CyberAware app shows promising educational results in terms of effectiveness. However, there was no mention about the cyber dangers in a home office environment and the app itself is targeted more for students and young adolescents, as such, the CyberAware app’s usage also remains unsatisfied in the context of this research.

4.5.3 Cyber Awareness Challenge

The Cyber Awareness Challenge is a free accessible browser game that is developed by the Defense Information Systems Agency for the Department of Defense (DoD) Chief Information Officer. The Workforce Improvement Program Advisory Council has a direct impact on the games’ content. Since 2012 the game is used by the DoD and other agencies to fulfil mandatory training requirements. Yearly updates keep the game up to date with regulations, sanctions and improvements [119].

The goal of the Cyber Awareness Challenge is to catch the hacker that is attacking federal government information assets in order to gain access to sensitive information. To be able to catch the hacker, players have to complete a series of tasks revolving around safe information assurance practices. For the majority of the tasks the player is sitting behind a desk in a virtual office with an interactive computer. Each day has a different set of tasks that need to be completed in order to progress to the next day. Tasks are divided into groups depending on the time and day, combined the tasks cover all the required information assurance content. A task can be split up into multiple smaller activities, solving all activities, will complete the task. Activities are mini games and simulations, simulations present the player with a scenario in which the goal is to select the safest course of action in a potentially endangering situation. Mini games challenge the player to apply information assurance concepts in an interactive context. The completion of activities grants the player points or, if incorrectly done, grants the hacker points. If the adversary gets too many points, the player will lose [120].

Through the completion of the game challenges, the player's learning progress is measured by the generation of performance data generated for each turn, which turns the game into an excellent measurement tool. Although the game is meant to be played by authorized users of the Department of Defense and Federal information systems, it can also be played for free from their website, which is accessible to anyone. The game is a great way to raise cyber awareness of office workers, but even though the game has yearly updates and revisions, it is still old fashioned. The Cyber Awareness Challenge is clearly a game and does not emerge the player; many people criticize and make fun of the game. There is also no inclusion of home office environment security situations, which makes this game unsuitable in the context of this research [120].

4.5.4 CybExer

CybExer, an Estonian company, developed a game-like cyber hygiene test, by which each participant must face multiple real-life situations and respond to a type of dangerous crisis in the virtual world. The participants are not graded in the traditional pass or fail way, but instead, after completion of the test, CybExer compiles the participant's personal risk analysis that includes their strengths and weaknesses. Based on the personal risk analysis recommendations are made to the participants on how to better protect themselves from cyber dangers. When the test is taken by employees of the same organization, a "drone-

mapped overview" of the weaknesses of the organization is generated, so it can be used by the organization's cyber security specialists in order to work on their weaknesses [121].

4.6 Conclusion

There is nothing new about games being used for educational purposes, as this chapter discussed some of the most popular cyber security educational games. Although there is a great variety of cyber educational games available, three relevant cyber security games were picked out and discussed. Each one of these games showed promising results in using video games to raise cyber awareness, two of which were even funded by government institutions. The analyzation of these games has revealed some key factors present in all three games, like rewarding players and keeping the player motivated. However great these games are, none of them focused specifically on security issues in home office environments, which reveals a gap that needs to be filled, especially with the increase of people working from home during the corona epidemic. In the next chapter the author discusses what elements are needed in a game to provide an efficient educational experience, so that they can be used in the concept of a new pilot game.

5 Methodology

5.1 Research design

The research was designed following the ADDIE model, ADDIE stands for the 5 phases in the development process: Analysis, Design, Development, Implementation and Evaluation. As the thesis is about a pilot game, the phases design and development will consist of suggestions by which the implementation phase is implicit. In the analysis phase the goals and objectives are constructed as well as research questions, aided by a survey on the focus group. The design phase will be made by creating the idea for a prototype using the analyzed information in the previous phase. Only a few suggestive game scenes will be created as suggestions for an active development scenario in the development phase. Since there is no actual prototype, there will no implementation phase [122].

The data was collected and analyzed using a mix of qualitive and quantitative research types. First the qualitative research was done using various text sources like articles, papers, studies, conference papers and books. Then a quantitative research was done using a survey with questions created from the information gathered in the qualitative research. The background theory and the analysis in the cyber security awareness chapter combined with the survey data will provide an answer to the first research question. The cyber security awareness chapter and the educational elements analysis combined with the survey data will provide an answer to the second research question. Finally, the games chapter analysis combined with the survey data will provide an answer to the third research question.

5.2 Research gap

During the qualitative research it became clear that there was a lot less information about cyber security at home offices. This could be due to the fact that before the covid-19 outbreak in 2020 working from home was less frequent. When analyzing home office

data, a lot of articles about working from home originated from this year, indicating that more and more people are paying attention to the risks when working from a home office environment situation. During the analyzation of the cyber awareness training and video game topics there was most certainly a lack of information in the home office department and certainly room for additional research. This research tries to make a contribution to the home office cyber security field by analyzing awareness training and video game topics in relation to a home office environment.

5.3 Focus group

The focus group of this research consists of secretaries or jobs similar to those of secretaries, because they are usually at the center of communication with other employees, CEOs and CFOs making them a valuable target for hackers. The focus group is international, since the surveyed secretaries are from Belgium. This means that although the survey is useful, it would most likely provide different results when held in Estonia. The secretaries were mostly part from medium-large companies with around 100 to 1000 employees, as the survey was launched in those kinds of companies. There was no age restriction, because age was not a factor, as secretaries had to work remotely independent of age and the author needed to have a large audience for the survey.

5.4 Survey

The survey is the quantitative research for the thesis, in which all questions were composed based on all analyzed information, while keeping the research questions in mind. The questions follow the structure of the previous chapters starting with cyber awareness questions leading up to educational questions and educational game questions. The questions were created in such a way for respondents to give the most exact answer reflective on the truth without a desired outcome. There are a few question types used in the survey: open-ended, multiple choice, likert scale, and matrix questions [123]. The amount of open-ended questions was limited due to the need for more specific and easier to quantify answers [124]. Before the survey was opened, it was piloted by 2 secretaries to make sure everything was understandable and relatable to secretaries. After that, the survey was opened from June 22nd until July 16th through direct contacts in one of the sub organizations of KYOCERA AERFAST in Belgium and on Facebook by one of the

participants in order to allow the survey to be spread. In total the survey was taken by 64 people with secretary-like jobs, although several Estonians were contacted, only Belgian people completed the surveys, meaning that replies are biased towards Belgian work culture. The analyzation of the survey results was done dividing the survey questions into their respective groups: categorical and ordinal [125]. The survey questions can be found in Appendix 2 – Survey.

5.5 Evaluation

The evaluation of the pilot game will be done based on an interview with 2 secretary professionals and one IT professional. The following questions will be presented:

1. What is the most important research question?
2. Do you feel the pilot game represents a realistic situation?
3. Thoughts about the storyline?
4. Any comments about the scenarios?
5. Do you feel like something is missing?

5.6 Limitations

Due to the time constraint the choice went to define a pilot game structure instead of creating an actual game, which takes a vast amount of time that far exceeds the amount given, while also having to do research. The pilot game could be improved and realized in collaboration with a game development company. Multiple Estonians were contacted, but did not respond when asked to fill out the survey, that is why the focus group only includes Belgian secretaries and that it is undeniable that the outcome of the survey will be biased to Belgian culture. The best way to improve the data results is to base the same study on a larger group of participants, preferably spread over multiple countries. The same counts for the evaluation interviews, if done on a bigger scale, the feedback would contribute more to the results. There are many different job functions employed at home during the covid-19 outbreak; the choice went to secretaries as they are usually at the center of communication making themselves a target for hackers. Research could be done to other home employed job functionalities in order to expand the research in new areas.

6 Results

There was no dominating age group as shown in Figure 4 and the results are almost evenly diversified over age.

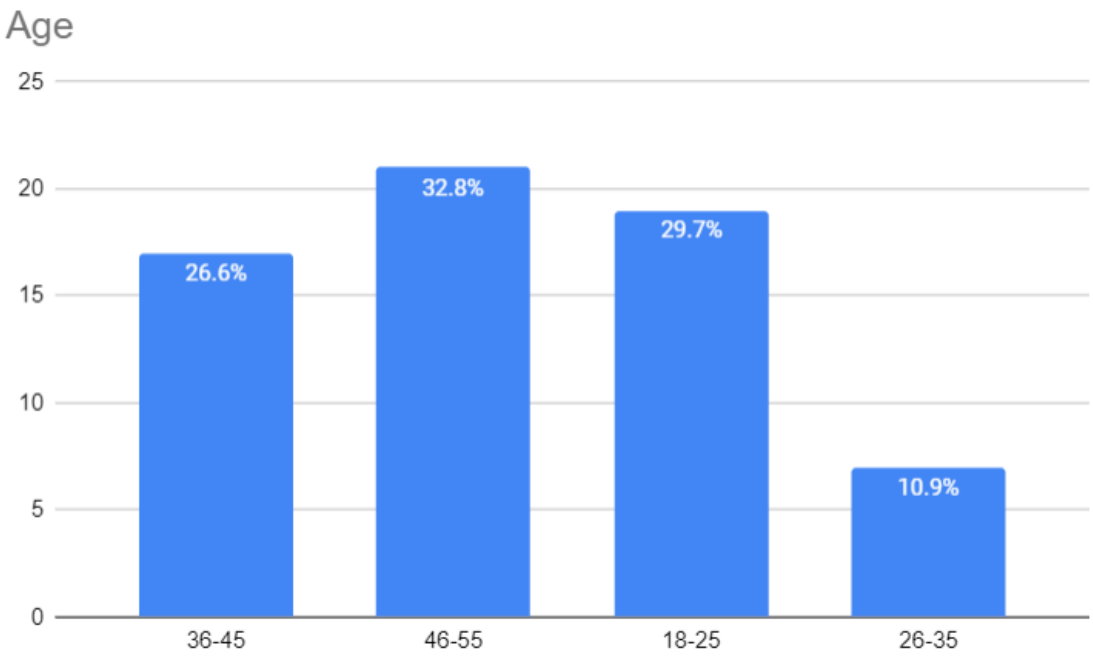


Figure 4. Age groups of secretary survey participants

As confirmed by the survey, cyber awareness and other IT related skills, like solving IT tasks or challenges, have an average competence of low or none in 80% of the cases as can been seen in Figure 5.

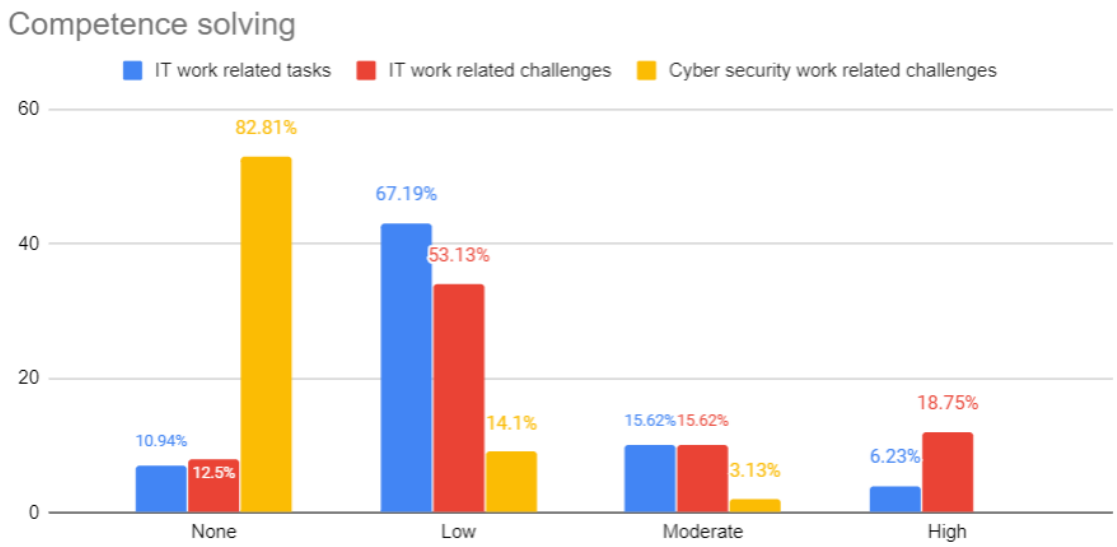


Figure 5. IT related competence of secretary survey participants

6.1 Common cyber security challenges in a home office situation for non-IT professionals

For the first research question the participants were required to select the devices and services provided by the organization to be used from home for work related tasks, as seen in Figure 6 and Figure 7. Although computers were provided in most of the cases (84.38%), the amount of smaller secondary devices used during work are not. Smartphones and web cameras were provided in less than half of the cases and in 15.63% of the cases the participant had no provided work devices. In this day and age, it should not come as a surprise that 100% of the participants had an e-mail service provided by work, however, when looking at the other provided services, there is a lot of work left to do. In 73.44% of the cases the company provided at least one cloud service and 60.94% had at least a chat application or internet provided. As discussed earlier, a VPN can seriously improve cyber security by using various encryption methods, which is so important, as only 62.5% of all the participants had a VPN service provided by the company.

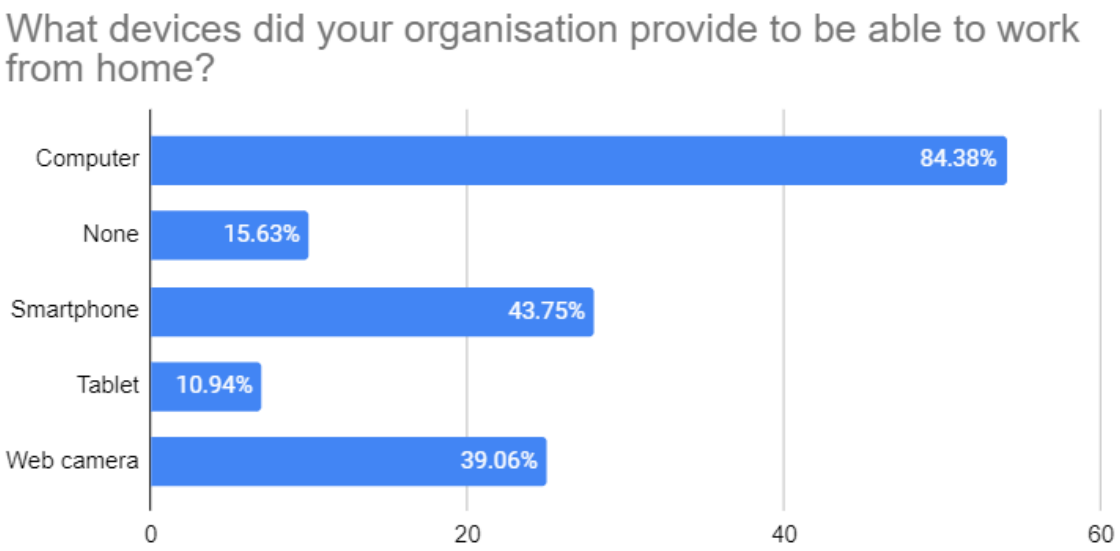


Figure 6. Devices provided by organizations from secretary survey

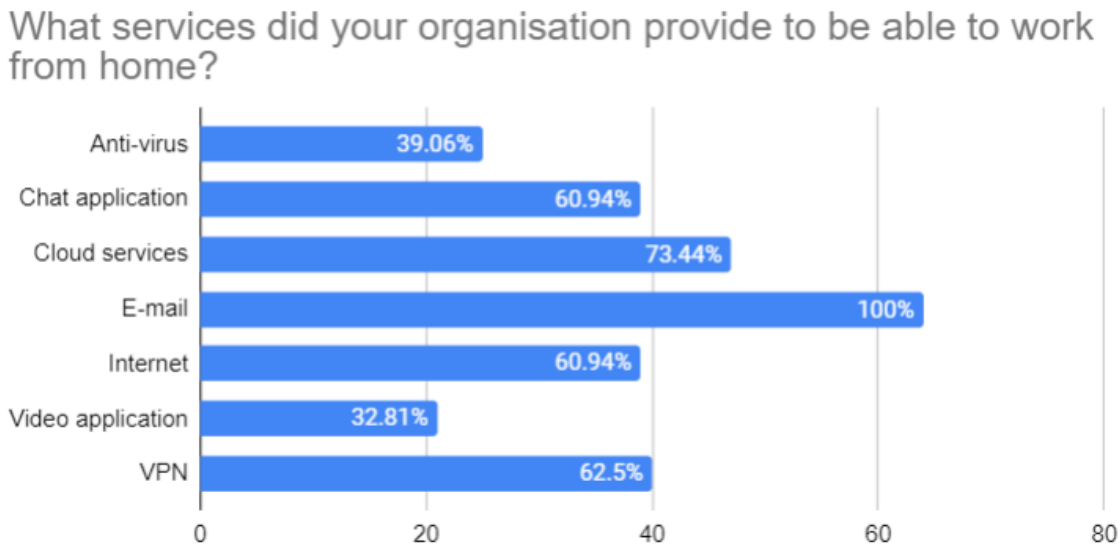


Figure 7. Services provided by organizations from secretary survey

Apart from the provided work devices and services, the participants had to select what personal tools and channels they used for work tasks and communication, as seen in Figure 8 and Figure 9. More than 67% used at least their personal smartphone or tablet to complete work tasks; both devices remain unmonitored by the company. In terms of personal communication channels, the top 3 were Facebook Messenger, Skype and WhatsApp. None of the personal communication channels and devices are monitored or have special company security measures and can pose security issues, which creates an opportunity to use them in game scenarios in order to demonstrate the security risks.

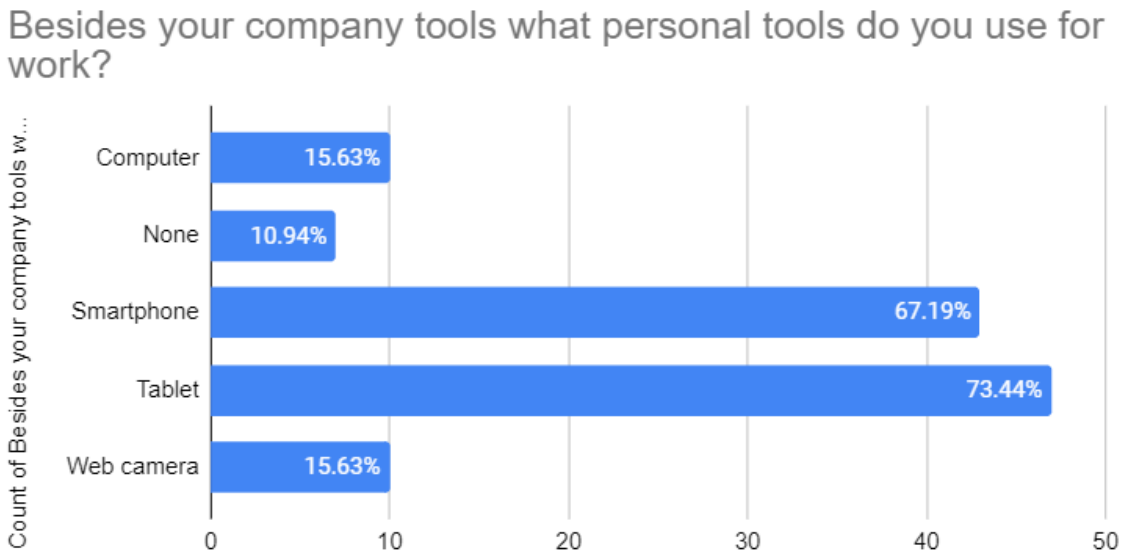


Figure 8. Personal devices used for work from secretary survey

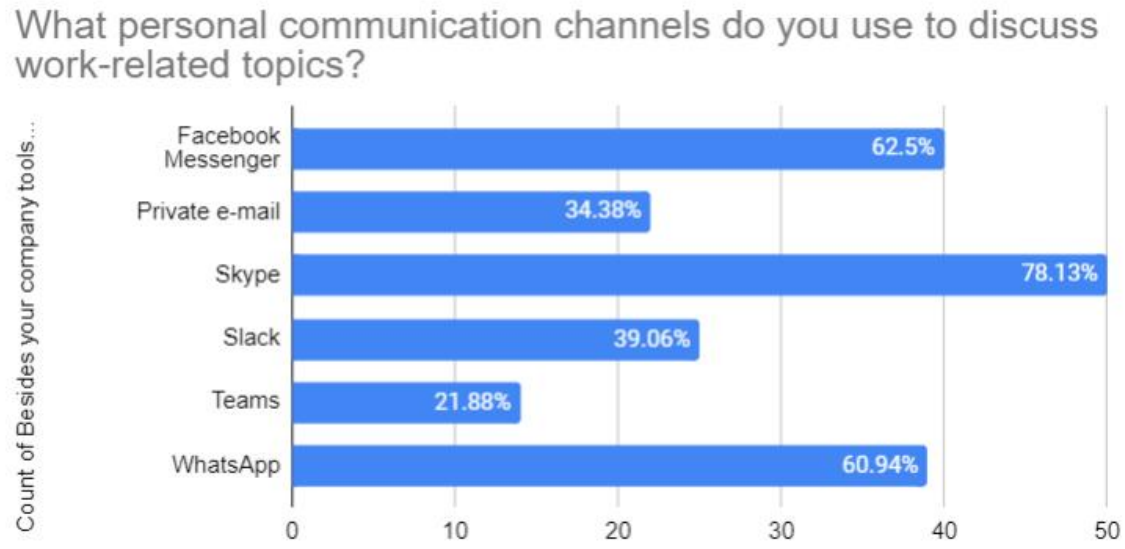


Figure 9. Personal communication channels used for work from secretary survey

The survey revealed that secretaries usually have direct access to the CEO/CFO through e-mail, phone or a video service like skype, which makes them a possible target for hackers wanting access to the CEO/CFO. The most frequently used web conferencing tools were Teams, Skype, Webex, Zoom and Whereby. Although the popularity of web conferencing, only 10% received a user manual and 15% had a mute mics rule. The remaining 75% had no rules set by the company whatsoever. On top of that, 62.5% of the participants stated to share their work device with at least their partner or children, which was not the case for the younger participants.

The participants had to select a likert scale option on 21 security statements to find out to which security risks less attention is paid. Out of those 21, the potential risks, with their respective combined agree percentages based on the risk it may pose in an unordered list, are determined as following:

1. I have once or twice used my personal e-mail to send out company related e-mails: 78.13%.
2. I have once or twice used the company mail to send out personal e-mails: 100%.
3. I always check e-mail attachments with an anti-virus tool: 21.88%.
4. I have a different password for each account: 39.06%.
5. I use strong passwords everywhere: 21.88%.
6. I use a password managing application: 0%.
7. I save passwords when my browser asks me to remind them: 40.63%.
8. I am usually logged in to both my company and personal accounts at the same time: 32.81%.
9. I am not easily distracted by personal home activities during active working hours: 65.63%.
10. I use my phone for personal matters during company hours: 67.19%.
11. I sometimes spend time on work related matters after official work hours: 100%.
12. I sometimes use the cloud to store work related matters: 100%.

6.2 Common delivery of cyber awareness to commoners

For the second research question the topic was cyber awareness training to see whether the participants were already trained and how they feel about cyber awareness training as seen in Figure 10. To get a better idea on the number of participants that had received some training, they were asked to select, which kind of trainings they had in the past 5 years. Out of all participants 34.4% had received no cyber security risk training at all, which is relatively high, although a surprising amount of 82.81% had received GDPR training within the past 5 years. 21.88% of the participants has been learning about cyber security/digital safety in their personal life.

Figure 10. Received company training related to cyber security risks in the 5 past years from secretary survey

The survey revealed that 100% of the participants was interested in improving either their IT related functionalities, IT related challenges, digital safety skills, or cyber security skills. When asked for the preferable way to be educated, 38% preferred to learn from a real-life practice example, 22.5% preferred to learn using a practical workshop, 18.6% chose for online courses including video examples, 14.7% wanted a video/simulation game experience and 5.4% preferred to just watch a video.

6.3 Gamification and video game scenarios that are useful for awareness training in cyber security

For the third research question not many participants seemed to choose for the video/simulation game. It were the rather younger participants between 18-25 that chose the video/simulation game option, which aligns with chapter 4.4 Challenges. When asked, what would capture their interest in an educational video game/simulation, all the answers were quite similar, the participants noted the usage of real-life examples and the visualization of dangers. The top 5 topics, which explain the threats of a home office, that participants wanted to be included in a video game, are:

1. Phishing
2. Password safety and management
3. Cloud data safety

4. Recognizing signs of a cyber threat and attack
5. Identifying harmful files

The reception of the video game was great, 89.06% of the participants voted positive, wanting to test the game after its development.

7 Discussion

How to write a discussion chapter: https://www.scribbr.com/dissertation/discussion/

7.1 Common cyber security challenges in a home office situation for non-IT professionals

What are the common cyber security challenges in a home office situation to non-IT professionals? As revealed in the introduction, cybercrimes is still a serious issue and on the rise. Although cyber security experts are creating solutions to combat these cybercrimes, cyber criminals usually target people, because they are the weaker part of the security chain. This fact does not change when employees start working in a home environment, especially during the covid-19 outbreak when most employees were forced to work from home. Employees had to suddenly change the way they operated, which introduced new attack vectors for cyber hackers. On top of that, due to the rapid shift, security teams had insufficient time to fully prepare all safety measures for each employee. Enforcing and controlling company security policies remotely proved to be difficult, especially with family members roaming around the house, who could in some cases use these same work devices or distract the employees. It was indicated by the theory that there was also a lack of company computers, although the survey results indicate otherwise for the secretary sector. When employees use their own personal devices for work, their installed applications, e-mail and social media, apps can make them more vulnerable. Not just any VPN will secure employees working from home, as for a company providing a VPN service to its employees to be able to connect remotely, it is important to make sure that the VPN is up-to-date to avoid publicly known exploits and to have the proper security measures in place. Even when employees use devices provided by the company, employees can share these devices with their partner or other family members, as was indicated by the survey, who do not follow any company policies. When working remotely, employees can get access to cloud services to storage work data. Using the cloud could introduce new vulnerabilities, as the security is in the hands of a third party. Phishing remains a big problem, in particular with spoofing to falsify the original sender's data. With the survey indicating that employees still use their personal e-mail to send out work related e-mails, phishing attacks could possibly be more effective when hackers can target the personal e-mail to gain access to company data. The increase

in remote video tools is being abused by hackers to send out fake video meeting invitations to trick employees. When companies do provide devices to work remotely, they often forget about smartphones and tablets which employees sometimes use to complete work tasks. Personal social media apps are unmonitored and as the survey indicates, often used to share work related messages. When employees are working from home, they have often have no other choice, when no chat or video applications are provided by the company. On top of that, the survey participants revealed, they usually had a direct communication line with the CEO/CFO through various communication channels like e-mail and skype. The data indicated that, in most cases, no clear company policies were set for the remote work. Thus, there are quite many cyber security challenges in a home office environment to non-IT professionals.

7.2 Common delivery of cyber awareness to commoners

How is cyber awareness commonly delivered to commoners? Most consider classroom-based awareness training the traditional way of training, although the data indicates this amount might not be what it used to be, which is good, considering the theory suggesting this way of educating is not the best for all adults. Visual pointers can be used, such as posters, to complement other methods of awareness training, but which are not sufficient when used solely. Simulated attacks are non-harmful attacks that can be used to create a lasting impact on the target(s), which is not always considered to be moral. The survey results show that a minority received training by the help of simulated attacks, while the majority of participants preferred to learn through this type of training. Computer-based training can be great for employees to learn at their own pace, but lacks the ability to actively change intentions and behavior. The data indicate that it was the largest selected option by the survey participants having received cyber awareness training, as well as the second most preferred type of training. Video games can be great to engage and motivate the player, but having to rely on previous gaming knowledge, can hinder the educational experience. Generalized gameplay could incorrectly represent company policies; the data show no participants having received this type of training, although a small percentage would prefer to receive cyber awareness training in this way. Group sessions are interactive and can actively change attitude and social norms towards cyber awareness, although generally perceived to be a great training method, no survey participants had received it. The majority of all participants indicated they had not received any cyber

awareness training in the past 5 years, which is a serious indication that some companies overlook employee cyber vulnerabilities.

7.3 Gamification and video game scenarios that are useful for awareness training in cyber security

What gamification and video game scenarios are useful for awareness training in cyber security? Gamification is a term used to indicate the usage of video game elements in non-gaming environments and systems. As such, gamification scenarios and video game scenarios refer to the same kind of scenarios. Using games as a learning medium, comes with a set of challenges, which are framing-related, learning-related, assessment-related and cost-related challenges. While not all challenges could be solved, it was not the goal of the thesis to perfect game learning. Through making the content iterative, the acquired knowledge can be more easily remembered. By dividing different scenarios over may be stimulated. Identifying the learning tasks and goals may prove difficult, but by using a survey the participants indicate knowledge gaps and low security awareness areas. The survey data indicate that most participants had an interest in play testing the game, in-case it would be fully developed that is, even the participants that did not select video games as their preferred learning medium. The top 5 topics that participants wish to see in video game scenarios are: phishing, password safety and management, cloud data safety, recognition of signs of a cyber threat or attack, and identifying harmful files. The data confirm that the useful scenarios to raise cyber awareness in cyber security depend on the demographic of the scenario target audience. The results shown here can apply in Belgium for the from home working secretaries, but might not for secretaries in Estonia or other.

8 Pilot game

A game concept is a vision of a game formulated in a descriptive text to create an easy way for involved parties, like publishers, investors and developers, to be on the same page. The game concept includes the core idea, art direction, platform and target audience. Since other concepts could be found, there is no clear official game concept structure. For that reason, Pluralsight's concept structure will be followed. Pluralsight is an online education company that hosts video training courses for creative and IT-professionals [126].

8.1 Core

The first thing that needs to be decided before a concept can be built is the genre that defines the entire game. For reasons discussed in Chapter 2.6, the genre of the game will be simulation in order to provide a realistic and practical educational experience.

As discussed in chapter 3.4 the game will be following the ARCS motivational model and case-based learning. The ARCS motivational model will be implemented as following, to keep the attention of the player the tasks will be short and simple, the task scenarios are based on the survey to make sure all topics are interesting to the player. As previously mentioned, the scenarios will be built up using survey results filled in by people with the same jobs, meaning that all the content will be extremely relevant and useful. To keep the confidence of the player high, the task difficulties will not be extremely, but task decisions will have real consequences to portray a realistic situation. Satisfaction will be upheld by rewarding security badges upon successful completion of certain tasks. The choice went for a badge system, as a sort of achievement system discussed in chapter 3.3.2, while still keeping the reward issues in mind of chapter 4.4. Case-based learning will be implemented by placing the player in real-world scenarios, all encapsulated by a realistic story line consisting of multiple virtual characters, with which the player will have to communicate. The learning process will be streamlined and self-guided with a help button providing useful tips, in-case the player is unsure of his actions to keep the scenarios as short and easy as possible to follow.

The player finds himself comfortably seated in front of his computer located at his home office with limited understanding of the dangerous cyber risks, to which his computer and

applications are exposed. The computer, being his main tool, will be equipped with a fully interactable desktop interface representing a modern-day desktop layout. The desktop has preinstalled applications like a browser, e-mail, password manager, social media, video, and chat. More applications become accessible when the story progresses in order to introduce new best practices and cyber risks. The goal of the game is to teach and guide the player into becoming more cyber aware by introducing new risk elements at various stages in the story.

The story is straightforward, the player must fulfill his daily secretary job duties (e.g. setting meetings, checking company documents, communication with office workers), which are presented by the hand of a simple task list presented on the desktop. While the player fulfills his daily duties inside the game, he will be exposed to cyber risks (e.g. phishing e-mails, virus attachments, dubious websites) and get realistic options when interacting within a risk environment (e.g. malicious e-mail; delete, scan attachments). If the player chooses the correct handling, he/she can receive a security badge for completing a particular task, but if the player chooses the wrong option, he will be attacked, of which the consequences depend on the type of attack (e.g. virus; computer will be compromised). After the attack consequences being played out, the player will be shown what he did wrongly and will be put back to the moment, before the bad decision was made. Not just attacks are demonstrated, but the player will also be shown how to use special safety applications (e.g. password managers, virus scanners) and will prompted to use those applications later on in different tasks. Future tasks can build on knowledge acquired in previous tasks (iterative) to stimulate memorization as discussed in 4.4.6 Learning goals.

8.2 Art

The name of the pilot game is CyberAware, although used by another application, this name is not trademarked here in Estonia, nor in Belgium. The game will be using a 3D style as it is specific to the simulator genre. The office that the player is in, will be fully visible by the player, as he will be able to look around the room. Other character models can appear in the room (e.g. child during confident video call). The 3D models should follow a light cartoonish style to avoid bringing in too realistic issues as discussed in chapter 3.3.4. The computer screen interface including icons and applications is slightly

cartoonish as well, in order to match the style of the world environment. Examples of this style for the main menu, office and desktop interface can be seen in Figure 11, Figure 12, and Figure 13

Figure 11. CyberAware pilot game main menu

Figure 12. CyberAware pilot game home office

Figure 13. CyberAware pilot game desktop interface

8.3 Platform and audience

The audience of the game is the focus group of the thesis, secretaries working from a home office environment. As for the platform, people have different operating systems like Linux, Mac OS and Windows, and in order to not exclude anyone, the game should eventually be running on the most used operating systems. The game should be as performant as possible to allow it to run on almost any semi-modern hardware configuration without the need of a dedicated video card.

8.4 Scenario examples

WhatGamesAre defines game scenarios as long-term tests that require several individual tasks in order to be completed. Although some games only have a single scenario, video games usually consist out of many [127]. The topic of the two example scenarios is determined by the survey results of the top preferred security awareness topics and each scenario will be described using in-game events. The final game would naturally contain way more scenarios, as otherwise the game would be too short; additional scenarios can include topics from the top preferred security awareness topic data or common cyber security challenges data.

8.4.1 Phishing attack

Task 1: Check computer

1. Player gets notification to log into his computer.

Task 2: Check email for work task

1. Player gets notified to check e-mail to find work task.
2. System sends 3 e-mails:
    a. The first e-mail is a phishing email without spoofing asking to login by clicking on the enclosed link.

        ➔ On link click go to event 3

    b. The second e-mail is the real e-mail originating from the boss to set-up a video conference by using the enclosed link.

        ➔ On link click go to event 4

    c. The third e-mail is a spoofed phishing e-mail originating from the (fake) IT-team to update the password after clicking on the link, because of a phishing e-mail wave.

        ➔ On link click go to event 3

3. Player gets credentials compromised and loses access to e-mail, the system visually shows a hacker using the credentials to contact other employees and sell the stolen credentials on the dark web.

        ➔ After visualization has been completed player goes back to event 2

4. Player receives job task notification

Task 3: Complete job task

1. System visually completes job task for the player.
2. Player gets notified that the task is completed.

8.4.2 Secure e-mail with password manager

Task 1: Install a password manager

1. Player gets notified to install password manager
2. Player gets notified to check for an e-mail originating from IT team about password safety measures.
3. Player finds the e-mail and clicks on the link that leads to a password managing website.
4. Player downloads the application from the website and installs it.
5. Player gets tasked to enter a master password to complete setup.
6. System remembers password so the player cannot forget it.

Task 2: Configure password manager

1. Player gets notified to open password manager from desktop and generate password for e-mail.
2. System enters master password upon player clicking in the password field.
3. Player uses simplified password managing interface to automatically enter email.
4. Player presses ‘generate password’ button .
5. System logs player out from e-mail.

Task 3: Use new password to log into e-mail

1. Player gets notified to use the newly generated password to log into e-mail.
2. Player presses ‘copy password’ button.
3. Player opens e-mail application and is welcomed by a login screen.
4. Player pastes e-mail and logs in successfully.

8.5 Evaluation interview

The first secretary professional selected the third research question as the most important one, as not all scenarios are useful and they should be easy to understand. She believed the pilot game to be realistic especially pointing to the phishing game scenario, since she has daily encounters with phishing e-mails. When asking about the use of video game elements, she believed it was a good way to bring out security vulnerabilities and tackle them. She liked the idea of using security badges to keep the attention of the player and keep him/her motivated. When asked if something was missing, she suggested the implementation of a dictionary to quickly search security terms, as she did not understand the word "spoofing". The second suggestion was to simulate a phishing attack through a chatbot, as she frequently uses them when contacting a customer agent from an airline. The final suggestion was to divide the game into multiple scenarios according to their difficulties from basic to expert, with expert modules involving more complex topics such as GDPR or data leakage.

The second secretary professional suggested her own combined research question, "how to teach and guide us (i.e. secretaries working from home) into becoming more cyber aware by introducing a pilot game with new unknown risk elements at various stages in the game story". She always finds games unrealistic, but the pilot game was found to be as realistic as possible, as the storyline was very realistic and the game tasks mimic her daily activities. She said it would be the fastest way for them to learn about cyber security and become more cyber aware. Her enthusiasm about the scenarios was great, as she mentioned, it would be a satisfying way to learn about those difficult topics. No suggestions for game additions were made, as she felt quite unsure about what to add.

The IT-professional opted to provide his point of view to two of the three research questions. On the first research question he replied that due to the corona-virus phishing attacks and VPN related attacks are on the rise, and if included in a scenario, it should have elements about the corona virus in the story. On the second research question, he replied that big companies usually let their employees take small tests to raise their awareness levels. He liked the fact that the person will be sitting physically in the game in front of his computer like in real life. When delivering in-game events, the way they are delivered to the player is important, as well as the sequence of game events, because it can make the story better. He mentioned RangeForce as a few story lines in their cyber

security awareness virtual machines; each machine has its own topic about what is going on. Although these machines are more specifically meant for IT-professionals, he said it would be good to take a closer look at them and study what them interesting. He likes the usage of badges to motivate the player, but he suggests looking into additional elements like a certificate the players can get upon completing the game. Another suggestion he made was to create a scenario around the botnet topic.

8.6 Conclusion

Using the previously researched theory and analyzed survey data, a pilot game has been structured with core elements such as a story, learning and motivational mechanics, art style and scenarios. The pilot game was then rated by two secretary professionals and one IT-professional to provide valuable feedback. The pilot game was well received and the feedback can be used to make further improvements.

9 Future work

The interviews were positive and some great suggestions have been made, which could be implemented in a future revision of the pilot game. Since the survey was only launched in Belgium, it could also be launched internationally and be divided per country to create localized scenarios that are most active in the respective country. Cyber security specialists could be contacted to provide further feedback and suggestions. The focus group of this thesis are secretaries working in a home office environment, but this group could be expanded by researching other job functionalities and branches out of the current target audience. A game development company could be contacted to check the viability of game elements, scenarios and features. Eventually a prototype could be built in collaboration with one of those companies to further research the user experience and impact. A company like Futuruum for example could use this idea and perhaps make use of the relatively new VR technology to further emerge the player in this cyber awareness game experience.

10 Conclusion

In this thesis the author tackles the problem of raising cyber awareness among non-IT professionals working in a home office environment using a pilot game concept. One of the main contributions are the data gathered from the focus group and the proposition of a pilot game using that data. First the current situation is researched on what is going on with cyber awareness around the world. Then cyber security awareness is defined and situated in the context of the research. Cyber security trainings are further researched on their effectiveness and common issues together with the cyber security risks in a home office environment. After that, some of the most frequently used learning models are researched together with the individual learning elements and their viability in a video game environment. Games are then defined and situated in the context of the research together with the challenges video games bring, when used as a learning medium and some of the most popular educational cyber games. By analyzing the awareness training and video game topics in relation to a home office environment this research has contributed to the research gap. A survey was done on the focus group to gain valuable data that could be used to introduce aspects and elements to the game. A detailed answer to the three research questions and a discussion of the research questions, in combination with the theory and survey data, provided a better insight to the elements a cyber awareness training video game could benefit from. The pilot game concept contains core elements such as story, learning and motivational mechanics, art style and scenarios. Additional propositions were then made for future improvements and for turning the pilot game into a real game, from which people could effectively learn. The pilot game concept was then proposed to professionals in the field and evaluated as part of the thesis.

11 References

[1] S. J. Lec, "Stanislaw Jerzy Lec Quotes," [Online]. Available: https://www.brainyquote.com/. [Accessed 10 February 2020].

[2] J. Clement, "Global digital population as of January 2020," 3 February 2020. [Online]. Available: https://www.statista.com/statistics/617136/digital-population-worldwide/. [Accessed 20 February 2020].

[3] "19 Alarming Cybercrime Statistics For 2020," Broadband Search, 2020. [Online]. Available: https://www.broadbandsearch.net/blog/alarming-cybercrime-statistics. [Accessed 29 May 2020].

[4] M. Cukier, "Study: Hackers Attack Every 39 Seconds," University of Maryland, 2007. [Online]. Available: https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds. [Accessed 29 May 2020].

[5] A. Patterson, "Overlooked Groups for Security Awareness Training," 25 September 2019. [Online]. Available: https://fowmedia.com/overlooked-groups-for-security-awareness-training/. [Accessed 15 February 2020].

[6] L. Hadlington, "Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom," *Open Access,* vol. 12, no. 1, p. 13, 2018.

[7] G. Kemper, "Improving employees' cyber security awareness," *Computer Fraud & Security,* vol. 2019, no. 8, pp. 11-14, 2019.

[8] M. Bada, A. Sasse and J. Nurse, Cyber Security Awareness Campaigns: Why do they fail to change behaviour?, 2015.

[9] A. T. A. S. Kartikay Mehrotra, "Cyber Risks Abound as Employees Shift From Offices to Homes," Bloomberg, 19 March 2020. [Online]. Available: https://www.bloomberg.com/news/articles/2020-03-19/working-from-home-a-cybersecurity-headache-for-employers. [Accessed 3 June 2020].

[10] S. Curry, "4 Major Cybersecurity Risks of Working From Home," Entrepreneur, 2 April 2020. [Online]. Available: https://www.entrepreneur.com/article/348346. [Accessed 3 June 2020].

[11] J. Gervais, "What is a VPN?," Norton, [Online]. Available: https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html. [Accessed 20 Juli 2020].

[12] "Cybersecurity Challenges for Remote Working," WebTitan, 23 March 2020. [Online]. Available: https://www.webtitan.com/blog/cybersecurity-challenges-for-remote-working/. [Accessed 3 June 2020].

[13] H. Murphy, "How remote working increases cyber security risks," Financial Times, 8 December 2019. [Online]. Available: https://www.ft.com/content/f7127666-0c80-11ea-8fb7-8fcec0c3b0f9. [Accessed 3 June 2020].

[14] C. Connley, "4 ways to be productive and avoid distractions when working from home," CNBC, 31 March 2020. [Online]. Available: https://www.cnbc.com/2020/03/31/4-ways-to-be-productive-and-avoid-distractions-when-working-from-home.html. [Accessed 3 June 2020].

[15] R. B. J. W. Daniel Schatz, "Towards a More Representative Definition of Cyber Security," *Journal of Digital Forensics, Security and Law,* vol. 12, no. 2, pp. 53-74, 2017.

[16] T. Sowell, Basic Economics (5th edition), New York: Basic Books, 2014.

[17] N. D.-T. R. P. Dan Craigen, "Defining Cybersecurity," *Technology Innovation Management Review,* pp. 13-21, 2014.

[18] "Security Awareness -- Definition, History, And Types," InfoSec Institute, [Online]. Available: https://resources.infosecinstitute.com/category/enterprise/securityawareness/#gref. [Accessed 9 May 2020].

[19] D. J. Joseph Boyce, Information Assurance: Managing Organizational IT Security Risks, Woburn: Butterworth-Heinemann, 2002.

[20] C. G. J. W. Andy Wu, "Security Awareness Programs," *Review of Business Information Systems,* vol. 16, no. 4, pp. 165-168, 2012.

[21] L. Irwin, "The 8 CISSP domains explained," it governance, 25 February 2019. [Online]. Available: https://www.itgovernance.co.uk/blog/the-8-cissp-domains-explained. [Accessed 27 July 2020].

[22] "CISSP Domain 1: Security And Risk Management- What You Need To Know For The Exam," INFOSEC, [Online]. Available: https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-and-risk-management/. [Accessed 27 July 2020].

[23] "CISSP Domain #2: Asset Security - What You Need To Know For The Exam," INFOSEC, [Online]. Available: https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/asset-security/. [Accessed 27 July 2020].

[24] "CISSP Domain 3: Security Engineering CISSP- What You Need To Know For The Exam," INFOSEC, [Online]. Available: https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-engineering/. [Accessed 27 July 2020].

[25] "CISSP Domain 4: Communications And Network Security- What You Need To Know For The Exam," INFOSEC, [Online]. Available: https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/communications-and-network-security/. [Accessed 27 July 2020].

[26] "CISSP Domain 5: Identity And Access Management- What You Need To Know For The Exam," INFOSEC, [Online]. Available: https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/identity-and-access-management/. [Accessed 27 July 2020].

[27] "CISSP Domain 6: Security Assessment And Testing- What You Need To Know For The Exam," INFOSEC, [Online]. Available: https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-assessment-and-testing/. [Accessed 27 July 2020].

[28] "CISSP Domain 7: Security Operations- What You Need To Know For The Exam," INFOSEC, [Online]. Available:

https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-operations/. [Accessed 27 July 2020].

[29] "CISSP Domain 8 Overview: Software Development Security," INFOSEC, [Online]. Available: https://resources.infosecinstitute.com/category/certifications-training/cissp/domains/software-development-security/. [Accessed 27 July 2020].

[30] "Four different types of security awareness training – and the pros and cons of each," CYBSAFE, 19 October 2018. [Online]. Available: https://www.cybsafe.com/blog/four-different-types-of-security-awareness-training/. [Accessed 25 Juli 2020].

[31] K. A. S. I. N. K. K. Bilal Khan, "Effectiveness of information security awareness methods based on psychological theories," *African journal of business management,* vol. 5, no. 26, pp. 10862-10868, 2001.

[32] G. S. Hussain Aldawood, "Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues," *Future Internet,* vol. 11, no. 3, pp. 1-16, 2019.

[33] "Cyber Security Awareness Training: What You Need to Know," Coretelligent, 19 February 2020. [Online]. Available: https://coretelligent.com/insights/cyber-security-awareness-training-what-you-need-to-know/. [Accessed 27 February 2020].

[34] "Security awareness training ROI," The Defence Works, 17 May 2019. [Online]. Available: https://thedefenceworks.com/blog/is-it-possible-to-calculate-an-roi-for-security-awareness-training/. [Accessed 28 February 2020].

[35] P. B. J. B. M. T. Lynne Coventry, "Using behavioural insights to improve the public's use of cyber security best practices," Government Office for Science, Northumbria, 2014.

[36] "National Cybersecurity Awareness Month 2019," 26 December 2019. [Online]. Available: https://niccs.us-cert.gov/national-cybersecurity-awareness-month-2019. [Accessed 25 February 2020].

[37] "What is ECSM?," [Online]. Available: https://cybersecuritymonth.eu/about-ecsm/whats-ecsm. [Accessed 25 February 2020].

[38] "Global Forum on Cyber Expertise," [Online]. Available: https://www.thegfce.com/about. [Accessed 2020 February 2020].

[39] D. Palmer, "Hackers are scanning for vulnerable VPNs in order to launch attacks against remote workers," ZDNet, 8 April 2020. [Online]. Available: https://www.zdnet.com/article/hackers-are-scanning-for-vulnerable-vpns-in-order-to-launch-attacks-against-remote-workers/. [Accessed 26 July 2020].

[40] N. Team, "Remote Access—Attack Vectors - Threats, Findings & Remedies," NCP, 2010.

[41] "Can VPNs Be Hacked? We Did The Research, Here's the 2020 Guide," vpnMentor, 1 June 2020. [Online]. Available: https://www.vpnmentor.com/blog/can-vpns-hacked-take-deeper-look/. [Accessed 26 July 2020].

[42] A. Zaharia, "300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends [2020] EDITION]," comparitech, 22 April 2020. [Online]. Available: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/. [Accessed 26 July 2020].

[43] C. Tennent, "What to Look for When Choosing a VPN," Internet Society, 24 October 2019. [Online]. Available: https://www.internetsociety.org/blog/2019/10/what-to-look-for-when-choosing-a-vpn/. [Accessed 26 July 2020].

[44] A. Jentzen, "Employees Take Risks When Using Corporate Devices for Personal Tasks," Proofpoint, 2 November 2018. [Online]. Available: https://www.proofpoint.com/us/security-awareness/post/employees-take-risks-when-using-corporate-devices-personal-tasks. [Accessed 26 July 2020].

[45] "6 security risks of enterprises using cloud storage and file sharing apps," Digital Guardian, [Online]. Available: https://digitalguardian.com/blog/6-security-risks-enterprises-using-cloud-storage-and-file-sharing-apps. [Accessed 26 July 2020].

[46] C. Barata, "Top 5 Threats To Email Security on Large Enterprises," Anubit Networks, 2 August 2018. [Online]. Available: https://www.anubisnetworks.com/blog/top-5-threats-to-email-security-on-large-enterprises. [Accessed 26 July 2020].

[47] "How Safe are Video Messaging Apps such as Zoom?," Security Boulevard, 31 March 2020. [Online]. Available: https://securityboulevard.com/2020/03/how-safe-are-video-messaging-apps/. [Accessed 26 July 2020].

[48] "BORED AND DISTRACTED EMPLOYEES ARE YOUR BIGGEST SECURITY RISK," 2|SEC, [Online]. Available: https://www.2-sec.com/2017/07/bored-distracted-employees-biggest-security-risk/. [Accessed 26 July 2020].

[49] Vanderbilt, [Online]. Available: https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/. [Accessed 28 July 2020].

[50] J. Burguillo, "Using game theory and Competition-based Learning to stimulate student motivation and performance," *Computers & Education,* vol. 2, no. 55, pp. 566-575, 2010.

[51] "Case-Based Learning," Yale, [Online]. Available: https://poorvucenter.yale.edu/faculty-resources/strategies-teaching/case-based-learning. [Accessed 11 June 2020].

[52] "PROBLEM-BASED LEARNING (PBL)," ILLINOIS CITL, [Online]. Available: https://citl.illinois.edu/citl-101/teaching-learning/resources/teaching-strategies/problem-based-learning-(pbl). [Accessed 13 June 2020].

[53] M. Brien, "What is Project Based Learning?," DefinedLearning, [Online]. Available: https://www.definedlearning.com/blog/what-is-project-based-learning/. [Accessed 13 June 2020].

[54] "ARCS MODEL OF MOTIVATION," Texas Tech University, Texas, 2017.

[55] "ARCS Model Of Motivational Design Theories (Keller)," Learning theories, 23 July 2014. [Online]. Available: https://www.learning-theories.com/kellers-arcs-model-of-motivational-design.html. [Accessed 7 July 2020].

[56] R. Wolverson, "Relatable," Merriam-Webster , [Online]. Available: https://www.merriam-webster.com/dictionary/relatable. [Accessed 10 March 2020].

[57] F. Groh, "Gamification: State of the art," *Proceedings of the 4th Seminar on Research Trends in Media Informatics,* pp. 39-45, 2012.

[58] "Real-life," Merriam-Webster, [Online]. Available: https://www.merriam-webster.com/dictionary/real-life. [Accessed 10 March 2020].

[59] G. W. Alaa AlMarshedi, "SGI: A Framework for Increasing the Sustainability of Gamification Impact," *International Journal for Infonomics,* vol. 8, no. 1/2, p. 9, 2015.

[60] "Rewarding," Cambridge Disctionary, [Online]. Available: https://dictionary.cambridge.org/dictionary/english/rewarding. [Accessed 13 March 2020].

[61] K. Kiili, "Procedia Computer Science," *The Design Principles for Flow Experience in Educational Games,* vol. 15, pp. 78-91, 2012.

[62] P. W. Penelope Sweetser, "GameFlow: a model for evaluating player enjoyment in games," *ACM Computers in Entertainment,* vol. 3, no. 3, pp. 1-24, 2005.

[63] K. H. Biyun Huang, "Do points, badges and leaderboard increase learning and activity A quasi-experiment on the effects of gamification," in *23rd International Conference on Computers in Education*, Hong Kong, 2015.

[64] C. S. Hao Wang, "Game Reward Systems: Gaming Experiences and Social Meanings," in *5th International Conference on Digital Research Association: Think Design Play, DiGRA*, Utrecht, 2011.

[65] "Practical," Reverso Dictionary, [Online]. Available: https://dictionary.reverso.net/english-definition/practical+experience. [Accessed 14 March 2020].

[66] "What is Active Learning?," Smartsparrow, [Online]. Available: https://www.smartsparrow.com/what-is-active-learning/. [Accessed 14 March 2020].

[67] D. B. D. R. Alina Zapalska, "Development of Active Learning With Simulations and Games," *US-China Education Review,* pp. 1548-6613, 2012.

[68] "video game," Dictionary.com, [Online]. Available: https://www.dictionary.com/browse/video-game. [Accessed 14 March 2002].

[69] "Realistic," Cambridge Dictionary, [Online]. Available: https://dictionary.cambridge.org/dictionary/english/realistic. [Accessed 16 March 2020].

[70] S. G. B. G. Richard Wages, "How Realistic is Realism? Considerations on the Aesthetics of Computer Games," *Entertainment Computing – ICEC,* pp. 216-225, 2004.

[71] "Naïve Realism," Merriam Webster, [Online]. Available: https://www.merriam-webster.com/dictionary/na%C3%AFve%20realism. [Accessed 16 March 2020].

[72] "Social Realism," Merriam Webster, [Online]. Available: https://www.merriam-webster.com/dictionary/social%20realism. [Accessed 16 March 2020].

[73] M. Mori, "The Uncanny Valley: The Original Essay by Masahiro Mori," IEEE Spectrum, 12 June 2012. [Online]. Available: https://spectrum.ieee.org/automaton/robotics/humanoids/the-uncanny-valley. [Accessed 16 March 2020].

[74] "Habit," Merriam Webster, [Online]. Available: https://www.merriam-webster.com/dictionary/habit. [Accessed 18 March 2020].

[75] B. X. Yin Bai, "Can You Form Healthy Habit? Predicting Habit Forming States through Mobile Phone," in *Proceedings of the 8th International Conference on Body Area Networks*, Beijing, 2013.

[76] D. Wohn, "The Role of Habit Strength in Social Network Game Play," *Communication Research Reports,* vol. 1, pp. 74-79, 2012.

[77] A. Blair, "5 games that actually make you more productive," Freelancers Union, 29 August 2014. [Online]. Available: https://blog.freelancersunion.org/2014/08/29/5-habit-changing-games/. [Accessed 18 March 2020].

[78] J. Zenn, "Designing Habit-Forming Games," GameAnalytics, 27 March 2018. [Online]. Available: https://gameanalytics.com/blog/designing-habit-forming-games.html. [Accessed 18 March 2020].

[79] E. G.-L. A. G.-C. Luis de-Marcos, "On the effectiveness of game-like and social approaches in learning: Comparing educational gaming, gamification & social networking," *Computers & Education,* vol. 95, pp. 99-113, 2016.

[80] S. Fisch, "Making Educational ComputerGames "Educational"," in *Proceedings of the 2005 conference on Interaction design and children*, 2005.

[81] M. Cristina, "Raising engagement in e-learning through gamification," in *The 6th International Conference on Virtual Learning*, Romania, 2011.

[82] "Uos "Sinu virtuaalne kodu"," [Online]. Available: http://www.ekuubis.eu/. [Accessed 9 May 2020].

[83] M. Gredler, "Educational games and simulations: A technology in search of a research paradigm," in *Handbook of research for educational communications and technology*, New York, MacMillan, 1996, pp. 521-539.

[84] S. Thiagarajan, "The Myths and Realities of Simulations in Performance Technology," *Educational Technology,* vol. 38, no. 5, pp. 35-41, 1998.

[85] K. Squire, "Video Games in Education," Massachusetts Institute of Technology, Cambridge, 2003.

[86] "Miniconomy at School," Miniconomy, 1 January 2002. [Online]. Available: https://www.miniconomy.com/en/edu/information.php. [Accessed 9 May 2020].

[87] "GAME ON: VIDEO GAMES ARE A STAPLE AMONG MILLENNIALS' MEDIA DIETS," Nielsen, 6 June 2019. [Online]. Available: https://www.nielsen.com/us/en/insights/article/2019/game-on-video-games-are-a-staple-among-millennials-media-diets/. [Accessed 10 May 2020].

[88] "Lockdown and loaded: coronavirus triggers video game boost," BBC, 6 May 2020. [Online]. Available: https://www.bbc.com/news/business-52555277. [Accessed 10 May 2020].

[89] "Game," Oxford, [Online]. Available: https://www.oxfordlearnersdictionaries.com/definition/american_english/game_1. [Accessed 10 May 2020].

[90] "Game," Merriam-Webster, [Online]. Available: https://www.merriam-webster.com/dictionary/game. [Accessed 10 May 2020].

[91] J. Arjoranta, "Game Definitions: A Wittgensteinian Approach," *Game Studies: the international journal of computer game research,* vol. 14, no. 1, 2014.

[92] "What's Tabletop Gaming?," OGRE'S DEN, [Online]. Available: https://theogresdengaming.com/tabletop-gaming/. [Accessed 10 May 2020].

[93] G. F. D. A. Lillian Frankel, in *Party Games for Adults*, Sterling, 2007, p. 7.

[94] J. Newman, Videogames, Routledge, 2004.

[95] N. Espocito, "A Short and Simple Definition of," in *Changing Views: Worlds in Play*, 2005.

[96] E. Adams, Fundamentals of Game Design, San Francisco: New Riders, 2013.

[97] V. Matthews, "The Many Different Types of Video Games & Their Subgenres," ID Tech, 12 April 2018. [Online]. Available: https://www.idtech.com/blog/different-types-of-video-game-genres. [Accessed 12 May 2020].

[98] D. I. F. Katie Seaborn, "Gamification in theory and action: A survey," *Int. J. Human-Computer Studies*, pp. 14-31, 2015.

[99] M. S. L. N. Sebastian Deterding, "Gamification. using game-design elements in non-gaming contexts," *Extended Abstracts on Human Factors in Computing Systems*, pp. 2425-2428, 2011.

[100] A. Leclerq, "10 Amazingly Successful Examples of Gamification," POTION , 08 June 2015. [Online]. Available: https://potion.social/en/blog/10-amazingly-successful-examples-of-gamification. [Accessed 15 May 2020].

[101] M. J. P. B. Tarja Susi, Serious Games – An Overview, Skövde: Institutionen för kommunikation och information, 2007.

[102] D. I. Xun Ge, "Designing Engaging Educational Games and Assessing Engagement in Game-Based Learning," in *Handbook of Research on Serious Games for Educational Applications*, Utah, IGI, 2016, p. 18.

[103] N. Whitton, Learning with digital games, vol. 15, New York: Routledge, 2009.

[104] K. Jørgensen, Gameworld interfaces, Cambridge: MA: The MIT Press, 2013.

[105] E. S. T. H. Timo Lainema, "Player-reported Impediments to Game-based Learning," *Harviainen*, vol. 1, no. 2, pp. 55-83, 2014.

[106] N. Whitton, Digital games and learning: Research and theory, New York: Routledge, 2014.

[107] D. Kim, "The link between individual and organizational learning," *Sloan Management Review*, vol. 35, no. 1, pp. 37-50, 1993.

[108] C. G. Robert Graham, Business games handbook, United States of America: American Management Association, 1969.

[109] T. Henriksen, "Extending experiences of learning games - or why learning games should be neither fun, educational or realistic," in *Extending experiences: Structure, analysis and design of computer game player experience*, Rovaniemi, University of Lapland, 2008, pp. 140-162.

[110] D. Myers, Play redux: The form of computer games, Ann Arbor: MI: The University of Michigan Press, 2010.

[111] T. Harviainen, "Critical Challenges to Gamifying Education: A Review of Central Concepts," in *Game On!*, Moscow, 2014.

[112] D. T. Yuri S., "How much does it cost to make a video game?," vironIT, 19 June 2018. [Online]. Available: https://vironit.com/how-much-does-it-cost-to-make-a-video-game/#:~:text=A%20game%20development%20process%20may,an%20action%2Dadventure%20video%20game.. [Accessed 12 July 2020].

[113] O. Pucek, "Hardware requirements and specifications for playing computer video games," HOW 2 DO, 25 September 2019. [Online]. Available: https://how2do.org/hardware-requirements-and-specifications-for-playing-computer-video-games/. [Accessed 3 August 2020].

[114] J. K. H. S. Juho Hamari, "Does gamification work? - A literature review of empirical studies on gamification," in *Proceedings of the 47th Hawaii International Conference on System Sciences*, Hawaii, 2014.

[115] "CyberSIEGE," Naval Postgraduate School, [Online]. Available: https://nps.edu/web/c3o/cyberciege. [Accessed 23 May 2020].

[116] D. C. I. Michael Thompson, "Active Learning with the CyberCIEGE Video Game," Naval Postgraduate School, 2011.

[117] C. I. M. T. T. N. Benjamin Cone, "A Video Game for Cyber Security Training and Awareness," *Computers & Security*, vol. 26, pp. 63-72, 2007.

[118] G. K. S. G. Filippos Giannakas, "CyberAware: A Mobile Game-based app for Cybersecurity Education and Awareness," in *International Conference on Interactive Mobile Communication Technologies and Learning (IMCL)*, Thessaloniki, 2015.

[119] "CyberAwareness Challenge 2020 for Department of Defense (DoD) DS-IA106.06," CDSE, [Online]. Available: https://www.cdse.edu/catalog/elearning/DS-IA106.html. [Accessed 25 May 2020].

[120] "Cyber Awareness Challenge," Serious Games Showcase & Challenge, 2012. [Online]. Available: http://sgschallenge.com/cyber-awareness-challenge/. [Accessed 25 May 2020].

[121] "Digital test by CybExer: a mission of patience to change the world," e-estonia, October 2018. [Online]. Available: https://e-estonia.com/digital-test-by-cybexer-a-mission-of-patience-to-change-the-world/. [Accessed 28 July 2020].

[122] "ADDIE Model," IntructionalDesign.org, 30 November 2018. [Online]. Available: https://www.instructionaldesign.org/models/addie/. [Accessed 29 July 2020].

[123] "Types of survey questions," Survey Monkey, [Online]. Available: https://www.surveymonkey.com/mp/survey-question-types/#open-ended. [Accessed 30 July 2020].

[124] "Independent Variables in Survey Methods," The Classroom, [Online]. Available: https://www.theclassroom.com/qualitative-quantitative-research-methods-8144495.html. [Accessed 30 July 2020].

[125] "How to Analyze Survey Data: A Comprehensive Guide," Qualaroo, [Online]. Available: https://qualaroo.com/marketers-guide-surveys/analyze-survey#:~:text=Besides%20response%20rate%2C%20the%20most,ordinal%2C%20interval%2C%20and%20ratio.. [Accessed 30 July 2020].

[126] "Creating a Game Concept: The First Step in Getting Your Game off the Ground," Pluralsight, 26 June 2014. [Online]. Available: https://www.pluralsight.com/blog/film-games/creating-game-concept-first-step-getting-game-

ground#:~:text=What%20Is%20a%20Game%20Concept,in%20order%20to%20create%20it.. [Accessed 22 Juli 2020].

[127] "Scenario," WhatGamesAre, [Online]. Available: https://www.whatgamesare.com/scenario.html#:~:text=Consulting-,Scenario,as%20Scrabble%20or%20Space%20Invaders.. [Accessed 2 August 2020].

[128] H. N. Security, "More than 99% of cyberattacks rely on human interaction," 10 September 2019. [Online]. Available: https://www.helpnetsecurity.com/2019/09/10/cyberattacks-human-interaction/. [Accessed 15 February 2020].

[129] S. X. Fan, "Video Games As Learning Tools—Fact or Fiction?," 22 Januari 2018. [Online]. Available: https://npjscilearncommunity.nature.com/users/34795-shelly-xuelai-fan/posts/29483-video-games-as-learning-tools-fact-or-fiction. [Accessed 15 February 2020].

[130] G. Strawbridge, "How to Promote Cyber Security Awareness in your Organisation," 4 June 2018. [Online]. Available: https://www.metacompliance.com/blog/how-to-promote-cyber-security-awareness-in-your-organisation/. [Accessed 15 February 2020].

[131] M. Holstein, "Playing Video Games Is Killing You," 26 June 2019. [Online]. Available: https://medium.com/tech-critical/playing-video-games-is-killing-you-cb99e6663c2a. [Accessed 20 February 2020].

[132] J. P. Gee, Are Video Games Good for Learning?, 2006.

[133] W. Ashford, "People top target for cyber attackers, report confirms," 5 September 2018. [Online]. Available: https://www.computerweekly.com/news/252448101/People-top-target-for-cyber-attackers-report-confirms. [Accessed 20 February 2020].

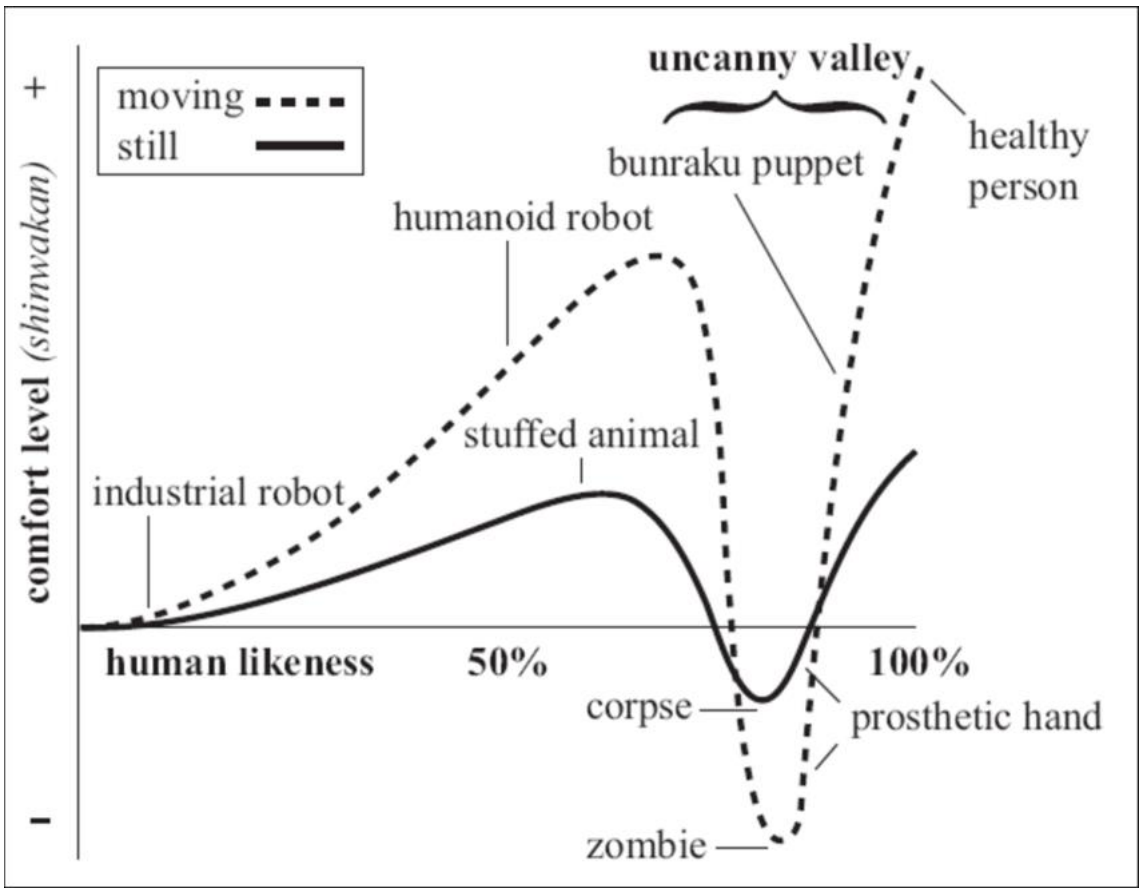
[134] M. Barr, "Student attitudes to games-based skills development: Learning from video games in higher education," *Computers in Human Behavior,* pp. 283-294, 2017.

[135] A. G.-V. A. H. Marta Martín, "Video games in teacher training: design, implementation and assessment of an educational proposal," *Informatics,* vol. 6(3), no. 30, pp. 1147-1154, 2019.

[136] "The Theory Of Game-Based Learning," gamelearn, [Online]. Available: https://www.game-learn.com/the-theory-of-game-based-learning/. [Accessed 1 June 2020].

[137] I. L. J. L. Zachary Collier, "Four domains of cybersecurity: a risk-based systems approach," *Environ Syst Decis,* vol. 33, pp. 469-470, 2013.

Appendix 1 – 'Uncanny Valley' Principle



Appendix 2 – Survey

Age *

- ○ 18-25
- ○ 26-35
- ○ 36-45
- ○ 46-55
- ○ 56+

Country *

Your answer

Job function *

Your answer

Rate your competence *

	None	Low	Moderate	High
Solving IT related work tasks	○	○	○	○
Solving IT related work challenges	○	○	○	○
Solving cyber security related work challenges	○	○	○	○

What device(s) did your organisation provide to be able to work from home? *

- [ ] Computer
- [ ] Tablet
- [ ] Smartphone
- [ ] Web camera
- [ ] None
- [ ] Other: _____

What service(s) did your organisation provide to be able to work from home? *

- [ ] Internet
- [ ] E-mail
- [ ] Cloud services (e.g. Google, Office)
- [ ] VPN (secure direct access to company network)
- [ ] Chat application
- [ ] Video application
- [ ] Anti-virus
- [ ] None
- [ ] Other: _____

Besides your company tools what personal tools do you use for work? *

- [ ] Computer
- [ ] Tablet
- [ ] Smartphone
- [ ] Web camera
- [ ] None
- [ ] Other: _____

What personal communication channels do you use to discuss work-related topics? *

- [ ] Facebook Messenger
- [ ] Skype
- [ ] WhatsApp
- [ ] VK
- [ ] Viber
- [ ] Discord
- [ ] Slack
- [ ] Private e-mail
- [ ] None
- [ ] Other: _____

Describe in short, how does direct communication with the CEO/CFO work in your company? *

Your answer

What web conferencing tools does your company use, if any?

Your answer

When videoconferencing did your company set any rules or regulation regarding on how it is used (e.g. mute microphone), what is visible or other?

Your answer

Has someone else from your family used your work device(s)?

- ◯ Yes
- ◯ No

With who are your personal devices/accounts shared with? *

- ☐ Friends
- ☐ Partner
- ☐ Children
- ☐ Parents
- ☐ Colleges
- ☐ No one
- ☐ Other:

Do you have administrative rights on your work device(s)?

- ◯ Ye
- ◯ No

Do you agree or disagree with the following statements? *

	Strongly disagree	Disagree	Agree	Strongly Agree
I have once or twice used my personal email to send out company related emails	○	○	○	○
I have once or twice used the company mail to send out personal emails	○	○	○	○
I use email filters (e.g. spam rules to automatically delete certain emails)	○	○	○	○
I always check the recipient e-mail address of an email before opening any attachments or links	○	○	○	○
I always check the link path before opening any attachments or links	○	○	○	○
I always check e-mail attachments with an anti-virus tool	○	○	○	○

Do you agree or disagree with the following statements? *

	Strongly disagree	Disagree	Agree	Strongly Agree
I use a VPN to access the company network from home	○	○	○	○
I use 2-factor authentication when possible	○	○	○	○
I have a different password for each account	○	○	○	○
I use strong passwords everywhere (+12 characters, numbers, special signs)	○	○	○	○
I use a password managing application (e.g. PasswordSafe)	○	○	○	○

Do you agree or disagree with the following statements? *

	Strongly disagree	Disagree	Agree	Strongly Agree
I save passwords when my browser (e.g. Google Chrome) asks me to remind them	○	○	○	○
I have separated personal and company social media accounts with different credentials	○	○	○	○
I have once or twice mixed up personal and company social media	○	○	○	○
I am usually logged in to both my company and personal accounts at the same time	○	○	○	○
I usually use the same browser for both company and personal tasks	○	○	○	○

Do you agree or disagree with the following statements? *

	Strongly disagree	Disagree	Agree	Strongly Agree
I am not easily distracted by personal home activities during active working hours	○	○	○	○
I make sure to be „undisturbed“ when discussing company related details with other employees	○	○	○	○
I use my phone for personal matters during company hours	○	○	○	○
I sometimes spend time on work related matters after official work hours	○	○	○	○
I sometimes use the cloud to store work related matters	○	○	○	○

Thinking back 5 years. Have you received company training related to cyber security risks, if so which ones? *

- [ ] By a lecturer
- [ ] Using a practice workshop
- [ ] Online course with videos and tests
- [ ] Video/simulation game
- [ ] Real life practice example (e.g. company launches controlled phishing attack to demonstrate)
- [ ] None
- [ ] Other: _____

Did you receive GDPR training in the past 5 years? *

- ( ) Yes
- ( ) No

Have you been learning about cyber security/digital safety in your personal life? *

- ( ) Yes
- ( ) Sometimes
- ( ) No

In what fields would you be interested to improve your skills in *

- [ ] Workplace IT related tasks (e.g. improving functionality)
- [ ] Workplace IT related challenges (e.g troubleshooting)
- [ ] Digital safety skills (e.g. digital hygiene)
- [ ] Cyber security skills
- [ ] None

How would you prefer to learn? *

- [ ] Lecturer
- [ ] Practical workshop
- [ ] Online course with videos and tests
- [ ] Video/simulation game
- [ ] Real life practice example (e.g. company launches controlled phishing attack to demonstrate)
- [ ] Reading a book
- [ ] Watching a video
- [ ] Participating in a play (improv theater or simulation in real life)
- [ ] Other: _____

If one would create a video game/simulation that explains the threats of a home office. What would be the three most important things to include content wise?

Your answer

What would really capture your interest in an educational video game/simulation?

Your answer

Do you know any good games that you would recommend to mimic a security awareness game?

Your answer

When do you think that a video game would not be solution for cyber security awareness training?

Your answer

Anything else to add?

Your answer

If you are interested in the results of the thesis or participate in an additional interview please leave your email here.

Your answer