Bachelor Degree Project

UNIVERSITY OF SKÖVDE

UTILIZING GAMES AS A TOOL TO INCREASE CYBERSECURITY AWARENESS IN ORGANIZATIONS

A Systematic Literature Review

SPEL SOM ETT VERKTYG FÖR ATT ÖKA MEDVETENHET OM CYBERSÄKERHET INOM ORGANISATIONER

En Systematisk Litteraturstudie

Bachelor Degree Project in Informatics with Specialization towards Network and System Administration - IT616G
Level ECTS
Spring term 2022
Date of Examination: 15/06-2022

Anton Karlberg
e19antka@student.his.se

Supervisor: Dennis Modig
Examiner: Ali Padyab

Abstract

Cybersecurity is an important aspect within organizations as threats are many and often not fully understood, which requires individuals employed within organizations to be educated. Training implementations to increase cybersecurity knowledge and awareness are varied in their methodology of teaching. This study has employed a qualitative systematic literature review of academic articles from five databases to investigate how games are utilized as a training tool to increase cybersecurity awareness in organizations. A thematic analysis was applied to the collected bibliography to extract the design mediums of the games and the subject areas that were trained, the target audience, and reported results were also analyzed. The analysis found that the games followed a collection of similar design themes, which were collected and categorized into three distinct categories consisting of card & board games, challenge games, and simulation games. By cross-analysis of the distinct categories and cybersecurity subjects trained, gathered results indicate that through different game design mediums different cybersecurity topics are favored, conclusions were then drawn on how games are applied in cybersecurity training within organizational environments.

Keywords: Cybersecurity, training, serious games, organizations

Sammanfattning

Cybersäkerhet är en viktig aspekt inom organisationer och hoten som existerar är många och ofta inte helt förstådda. Vilket skapar behovet att utbilda individer inom organisationer om cybersäkerhet. Utbildningsimplementationer kommer i många former och varierar i sin metodik i att lära ut. Denna studie har brukat en kvalitativ systematisk litteraturstudie av akademiska artiklar inom fem databaser för att undersöka hur spel används som träningsverktyg för att utöka cybersäkerhetskompetens inom organisationer. En tematisk analys applicerades på den samlade bibliografin för att extrahera spelens designstrategier och vilka områden av cybersäkerhet som blir utlärda samt målgrupp och resultat. Analysen visade att spel följde en samling av liknande teman av design som kategoriserades i tre distinkta kategorier bestående utav kort & brädspel, utmaningsspel och simulationsspel. Genom korsanalys av de distinkta kategorierna och område av cybersäkerhet som tränades indikerade samlade resultat att skilda designstrategier föredrar utlärning av olika cybersäkerhetsområden. Slutsatser formulerades av dessa resultat som ger väg till hur spel appliceras för cybersäkerhetsträning inom organisatoriska miljöer.

Nyckelord: Cybersäkerhet, träning, seriösa spel, organisationer

Table of Contents

1 Introduction

Cybersecurity is a constant theme in large sectors of society today and as IT infrastructure is expanding so do the areas vulnerable to threats. In businesses and organizations, it is of utmost importance that high levels of cybersecurity standards are met and upheld to follow privacy laws and secure their assets. According to research most incidents regarding cybersecurity-related attacks in businesses are caused by the employees that have been exploited by attackers through social engineering attacks (Chowdhury & Gkioulos, 2021a). Vulnerabilities in cybersecurity can lead to devastating damages, as seen in the US where $121.22 billion are lost each year, with further losses of £27 billion annually in the UK (Hendrix et al., 2016; Salahdine & Kaabouch, 2019). Humans have the rather unfortunate tendency to accept most communications at face value which leaves them open to social engineering attacks that are becoming more frequent due to the lower level of difficulty in performing a social engineering attack compared to other cyber-attacks (Bullée et al., 2015; Ghafir et al., 2016). To combat this weakness, training of the employees at businesses and organizations has to be implemented as it has been shown in research that the risk of breaches using social engineering attacks will be reduced with training (Bullée et al., 2015). There exists a multitude of ways to teach such as lectures, videos, seminars, etc. however in recent years games have become a favorable training method to increase cybersecurity awareness among employees.

Games come in many forms, both digital and nondigital, their design can vary in multiple aspects, including gameplay, artistic design, sound design, story, and much more. Due to the flexibility of games a wide range of topics can be covered if it is used as a training tool to increase cybersecurity awareness. The games can be highly specialized or cover more ground by being more general in what threats they aim to educate about.

Games have in recent years been utilized as a training tool in education, from kindergarten to universities, to educate in many different areas, including cybersecurity (Hendrix et al., 2016). There exist a plethora of articles researching games as a tool to teach cybersecurity and increase their awareness of it to students, as well as literature reviews that collect and analyze them. A lesser researched area is the utilization of games to teach cybersecurity in the workplace and literature reviews that analyze them are to the knowledge of the author non-existent. This work aims to further the knowledge of how cybersecurity awareness can be increased in organizations by utilizing games, both digital and non-digital, and giving a deeper dive into how they are designed to disperse their knowledge to a working audience. This work will be conducted in the form of a Systematic Literature Review (SLR) as this method will allow

for a widespread search of articles that are relevant to the topic utilizing multiple databases and predefined selection criteria. Selected articles will then undergo further analysis to gather data using thematic coding as explained by Braun and Clarke (2006) to conclude the selected articles.

In this work, the current landscape of games that are utilized as a training method to increase individuals' cybersecurity awareness that is employed within corporations, organizations, and businesses will be mapped and discussed. Furthermore, the games' intentions, design, target audience within an organization, and the results of utilizing them to increase cybersecurity awareness will be discussed.

In chapter 2 the background to this work is discussed and brief introductions to the building blocks of the topic are given as well as related works. In chapter 3, the aim of the research as well as the work's practical limitations are given. Chapter 4 describes the methodology used, including the planning phase, execution phases done during the article selection, and the data analysis. Chapter 5 details the implementation of the methodology. Chapter 6 details the analysis and the results of the selected articles. In chapter 7 the conclusions that are drawn from the literature review process are discussed. In chapter 8 the reviewing process, results, future research as well as ethical and social impacts of the work are discussed.

2 Background

This chapter will discuss and define the concepts of cybersecurity and what it entails and how it can be threatened by exploiting humans and technological vulnerabilities, as well as detailing games as a tool to teach. The threats that are discussed are the common ones that training typically aims to combat. It will also briefly discuss related works to give further motivation as to why the topic is relevant to be researched.

2.1 Cybersecurity

Cybersecurity is the practice of protecting systems and information from attacks and preserving confidentiality, integrity, and availability (CIA), and increases in importance as the IT market grows (Jang-Jaccard & Nepal, 2014). Cybersecurity encompasses a large sector of organizations, from the password security on a secretary's computer to the source code made by a developer, and to the detection and prevention systems in the network. The concept of cybersecurity therefore also grows in importance as the attack surface becomes larger which is threatened by attacks from multiple sources that target both humans and digital systems. According to research by Hendrix et al. (2016), the UK loses £27 billion annually due to cybercrime that exploits vulnerabilities in cybersecurity, in their research, they state that these losses can be reduced using education to increase cybersecurity awareness.

2.2 Cybersecurity Threats

Understanding and training to protect cybersecurity by increasing awareness and knowledge of threats and their sources as well as their targets is a necessity. Humans are targeted by social engineering threats which consist of a large collection of attacks that utilize human psychology to gain unauthorized access to systems or to steal information such as passwords, or Personally Identifiable Information (PII) (Krombholz et al., 2015; Smith et al., 2013). Cybersecurity can further be threatened by attacks that are digital in origin and target networks and systems to illegally retrieve information or cause larger amounts of downtime, threatening confidentiality, integrity, and availability (CIA) (Kim et al., 2012). The following subchapters will detail the common threats to organizations to further strengthen the argument of why cybersecurity awareness training is required.

2.2.1 Social Engineering Threats

To further understand social engineering and how it can threaten cybersecurity, the most common social engineering threats that exploit the vulnerabilities caused by a lack of cybersecurity awareness in employees will be discussed and reviewed.

Phishing is the practice of sending fraudulent emails that appear to be legitimate to fool users into revealing personal information, such as passwords, bank information, and other sensitive data. In organizations, phishing emails are utilized by attackers to gain insight or access to unauthorized parts of a network. Phishing attacks have shown themselves to be successful whilst being easy to distribute, however increasing awareness of phishing attacks through training has also shown itself to be successful (Jansson & von Solms, 2013). Employees at businesses are typically a prime target for these kinds of attacks, this can range from a common desk worker to a higher-up executive, an attacker can target their phishing attacks, which is commonly known as spear phishing (Chiew et al., 2018).

Phishing attacks can utilize other forms of technology to spread and deceive users, in recent years vishing (Voice phishing) and SMiShing (SMS phishing) have become more prominent as a mode of attack as users have greater knowledge of the traditional phishing attacks. Vishing utilizes phone calls, with techniques such as fake caller ID to achieve similar aims to phishing whilst SMiShing utilizes text messaging on phones, a common example of this is sending messages claiming that there is a delivery from a shipping company that can be picked up using a link within the message (Yeboah-Boateng & Amanor, 2014).

Baiting attacks commonly known as road apples are utilized by placing seemingly harmless USB drives, or other computer peripherals in public in hope that a victim will take them and insert them into a machine, thus allowing the perpetrator to finalize their attack by installing some kind of malware on that machine through the peripheral (Salahdine & Kaabouch, 2019). These attacks exploit unaware victims as most people are curious and if not educated would most likely pick up the planted item. Pretexting invents scenarios to convince victims to give away personal information, password, or other types of information that should remain secret. These attacks are often done in direct communication both digital and non-digital, attackers can use the knowledge gained to stage further attacks on an individual or company the victim works for (Weber et al., 2020). Tailgating tricks victims into allowing an unauthorized person into a building, this type of attack is also known as piggybacking as an attacker will position themselves by a door they cannot pass and follow a victim through when the opportunity arises (Salahdine & Kaabouch, 2019).

2.2.2 Network and Cyber Threats

Networks and systems are the core of any organization as without them they cannot function considering the inter-connectivity of the world today. Understanding common threats that exist to digital systems and how to defend against them is essential.

Malware attacks are a subset of cyberattacks that target systems to disrupt the CIA, through several means some of which are, ransomware which takes systems hostage,

worms that spread through networks to destroy or steal information, and spyware which gathers information (Razak et al., 2016). These pieces of software can be distributed into systems and networks through several means, including several social engineering strategies, and hacking security systems. Further attacks include denial of service attacks which exploit weaknesses in networks to disrupt the availability of organizations' systems and services (Carl et al., 2006). Additional network threats include man-in-the-middle eavesdropping attacks to intercept and scan messages between parties (Mallik, 2019).

2.3 Serious Games

Games have always had a place in society for entertainment, there are often aspects of them that can be used for education however they are usually emerging as a byproduct due to the structure and rules of the gameplay, these are quite common occurrences in older games such as chess, go and shogi which develops a players analytical and problem-solving skills (Aciego et al., 2012). In the last 50 years, the term "Serious Game" (SG) has gained relevancy and these SGs are created to educate players first with entertainment being secondary as a way to keep player retention and increase their motivation for learning (Djaouti et al., 2011). Another term has also recently gained popularity, that being, "Game-Based Learning", which is defined as "gameplay with defined learning outcomes" (Plass et al., 2015). Game-based training, therefore, adds an aspect of fun through the games which differs from gamification, which is the practice of applying game design elements, mechanisms, and thinking to non-game activities to increase participant retention to add a competitive environment to the training (Al-Azawi et al., 2016). Gamification, therefore, acts as an extension to regular training methods whilst game-based training is a fully-fledged unique method.

Properly made SGs have proven themselves to be an effective way of disseminating educational information to their players, and have been implemented in many environments, some being in medical education or the IT sector (Graafland et al., 2012; Zhonggen, 2019). Cybersecurity awareness training has been a relevant topic since the Internet became mainstream. Professionals have since then attempted to bring this topic to the masses through seminars, workshops, and other training methods. These have shown positive results. However, in recent years SGs have become a favorable option to inform individuals about cybersecurity awareness due to the engagement they can employ from the trainees with the ease of implementing them after creation (Chowdhury & Gkioulos, 2021a; Jin et al., 2018; Skarga-Bandurova et al., 2016). One SG that shows the potential of SGs as a reputable training tool within cybersecurity awareness training is "Anti-Phishing Phil" which aims to combat phishing through the gameplay which consists of the player controlling a fish that has to eat worms (good URLs) whilst avoiding the worms attached to hooks (bad URLs) (Sheng et al., 2007).

2.4 Related Works

To the knowledge of the author, there currently exist no literature reviews that study the types of games that are utilized, how they are utilized, their aim, their target audience within organizations, and the results of using the games as a method to increase cybersecurity awareness. Similar works exist, however, that aim at other aspects of cybersecurity awareness and will be discussed in this chapter.

In their literature review, Quayyum et al. (2021) discuss, review and map the different training methods that currently exist to increase cybersecurity awareness for children, further their work focused on current cybersecurity risks for children and approaches and theories for raising awareness. The authors reviewed a wide variety of training methods, including games, which were reported to have a modicum of positive results where one game resulted in increased knowledge after gameplay but another showed no significant results when teaching already known concepts. They further reviewed the theories and models used in the studies of the training methods, the theories involved different kinds of psychological or cognitive processes in children and individuals, such as the resilience theory, which is the theory of building resilience through risk exposure (Fergus & Zimmerman, 2005). The training methods reviewed as earlier stated involve common methods such as informative videos, comics, curriculum, interventions, gamification, warnings, negotiation within families, and mobile apps as a one-stop solution.

In the work done by Chowdhury and Gkioulos (2021a) they seek to establish the different cybersecurity training methods that are currently in use in critical infrastructure with a focus on the aviation, energy, and nuclear sectors. The analysis of the training methods found in the articles by the authors was broad and included most types of training, such as training frameworks, gamification, game-based approaches, and lab environments, these were later examined for their comprehensiveness and effectiveness as a way to further research and find which methods had a higher success rate within critical infrastructure, as well as the aviation, energy and nuclear sectors. The authors found that regarding games as a training tool engagement levels were high along with positive results from the practical application due to the gameplay and aided in the ability to develop team skills and paired with traditional training would elevate cybersecurity awareness training to a new level.

In their paper, Chowdhury and Gkioulos (2021b) aimed to find and identify articles that have researched the topic of competencies and skills required for critical infrastructure and cybersecurity protection as well as how these competencies are to be achieved. The authors state that there is no set agreement of which skills are necessary but, in their article, they have found that a common theme exists and through that, they have mapped out a baseline of skills. The authors found in their literature search a few

games created with the purpose to increase competencies, they reported in their findings how the games are a cost-efficient and flexible way of teaching with positive outcomes, but also their limitation of topics that can be taught unless the game is further developed.

Aldawood and Skinner (2018) describe in their article different social engineering cybersecurity threats along with implemented solutions to raise awareness against said threats, the article has a broad focus and discusses multiple solutions which include a game, they identify that the utilization of games along with security awareness programs are an effective method to increase awareness as it allows the players to experience the threats first hand whilst doing regular activities in a safe virtualized environment. This allows for the players to develop a sense of mistrust and suspicion regarding possible threats.

In a study by Khando et al. (2021), the current state of information security awareness (ISA) methods and factors existing for employees' ISA awareness are reviewed, games being one of these methods. Through the authors' review of the collected articles, they found that training in the form of playing games is a suitable solution in increasing employees' ISA level in the private sector due to how they can be customized to fit the needs of the particular ISA training, this allows for mastery and progression which further engages players increasing ISA. They further report that games in the public sector also followed this trend, the games they found targeted the healthcare sector and introduced the topics regarding phishing, web use, malicious codes, and password protection. The private sector game was still in its prototype stages but showed promising results and both games utilized similar designs.

Hendrix et al. (2016) performed a literature review to find out if serious games were suitable for cybersecurity training, in this study the authors identified 28 articles that discuss cybersecurity training games and their effectiveness as a training medium. They found that most research articles and their proposed games focus on raising awareness within the general public, and address security within networks, phishing, and end-user PC protection. They further find that few address security professionals, most articles have a positive result but some were unclear or nonexistent. They further researched available products available for cybersecurity training and found that most are aimed at children, students, and teachers, with only one being aimed at companies and two at the health sector. Their article concludes with the statement that research and games that target IT infrastructure and organizations are lacking within their search results, with few available that have not yet been tested rigorously, it further concludes that with the research results available only immediate results are shown, this shows positive indicators, however, but further research is required to understand the long-term impacts.

3 Problem Definition

This chapter aims to provide insight into the general problem area, furthermore, it will motivate as to why utilizing games as a training tool to increase awareness in organizations is targeted by this thesis work. The following subchapters will discuss and establish the aim of the research along with the purpose and goal of the article as well as the limitations that exist in the paper.

Currently, there is a multitude of training methods to increase cybersecurity awareness in organizations with each having a varying degree of effectiveness, understanding their effectiveness is an important factor when choosing a method of training for a company (Chowdhury & Gkioulos, 2021a). Through the research on the topic of games as a tool to increase cybersecurity awareness in corporations as well as other organizations or associations, further information will be available to researchers and personnel that require it, more on this in subchapter 3.1.

The increased use of computers in organizational environments further cements the idea of increasing cybersecurity awareness, employees are always threatened by, to them, unknown cybersecurity threats and typically they have next to no knowledge about it, a well-intentioned employee can cause high amounts of damage by simply clicking on the wrong URL (Gundu, 2019). This of course can be remedied through training and has seen positive results in the trainees and a direct positive correlation to the organization they work for (Chowdhury & Gkioulos, 2021a).

As described in the chapter for related works, previous research has only been used to chart the current landscape of training methods in general, leaving a lot to be desired about how games can be utilized in organizational environments.

3.1 Aim and Purpose

This research work aims to investigate and map the current landscape of available cybersecurity training games used to train individuals employed by organizations and gain an understanding of how these games are utilized to increase the cybersecurity awareness of individuals. Awareness is increased through gaining knowledge of cybersecurity threats, vulnerabilities, defenses, tactics, and any related building blocks of cybersecurity. Further, the study also aims to find out what the aim or goal the games want to achieve and finally who the target of the game is within an organization, and if available, how effective they were in training their targeted audience.

The aims can thus be separated into categories, these being the following:

- The games & their design

    - What games exist, how are the games designed, and in what style have they been made.
- Target audience within an organization
    - What audience is the game aimed at.
- The aim of the game
    - Aims to find out what the core aim of the game is, and what exactly the game wants to teach within cybersecurity awareness to the players that play the game.
- Result
    - Aims to find out what the results of the game are, how have the players been affected by the game, have their awareness increased, how did they feel about the game, and did they feel it was an effective and fun method of learning.

Through this work, the purpose is to collect and analyze the currently existing research to allow for further increased knowledge and awareness regarding cybersecurity awareness in businesses and how games are utilized to increase said awareness. The practical purpose of the finished work is to allow for a foundation to be built upon which further work within this research area can utilize to develop new games or build upon to fork the games to include further topics or if businesses want to implement cybersecurity awareness training through games they can either use this article to find a game that fits their criteria or help in the development of a completely new game.

With this in mind the purpose and aim of the work can be summarized with the following research question:

> *How are cybersecurity training games utilized to increase cybersecurity awareness in individuals employed within organizations?*

3.2 Delimitations

The main limitation in this work is the area it covers, it only includes games, both digital and non-digital, and how they are utilized to increase cybersecurity awareness in organizations, further limitations include the targeted audience which in this article extends to working personnel in organizations, and not on students or others. This work will neither delve into deep game theory nor game design as it is outside of the scope of systems administration.

4 Methodology

Throughout this chapter, the method used in the paper to conduct the review is explained in detail, it will also discuss and motivate as to why this method was used.

As previously mentioned the goal of this article is to identify games that are being used as a tool to increase cybersecurity awareness and to discuss and review their design, target audience within an organization, the aim of the games, and their results to further the accumulated knowledge and act as a pool of information to aid future research or implementations of cybersecurity training. With this in mind examining existing research literature for relevant and useful information in the form of a systematic literature review becomes the most topical way of conducting this work as systematic literature reviews focus on evaluating and interpreting all available research that is relevant to the topic (Kitchenham, 2004). Other ways of research such as interviewing researchers could be a possible method but pale in comparison to the effectiveness of the possible ways of research.

In her work Kitchenham (2004) argues that there are several reasons to conduct systematic reviews, with the more common ones including the summarization of existing evidence, identifying gaps in current research to further investigation and knowledge, and providing a framework and background for new research.

To find the largest number of articles that pertain to the topic a systematic rigorous standard has to be set and followed, this is what is known as a systematic literature review (SLR), using SLRs also allows for the reproduction of the process, as each part of the process is properly documented and described within the methodology of an article (Okoli & Schabram, 2010). According to Santos and Silva (2013), SLRs are typically employed in works that aim to guide or help future research, which is one of the aims of this study. Furthermore, the work done during an SLR requires certain amounts of rigor and through the requirements put on SLRs, a proper academic piece will arise, as it has gone through the proper motions of synthesizing the available material and reaching a conclusion (Okoli & Schabram, 2010). In essence, employing an SLR for this work will allow for the openness of the methodology, which in turn creates a replicable study that others can follow to prove its validity. As the purpose of this work is to increase the accumulated knowledge and act as a starting point for further research, it is important to ascertain that all available articles researching games and how they are utilized to increase cybersecurity awareness of individuals within organizations are gathered and analyzed thoroughly, thus a systematic literature review was chosen for this thesis.

4.1 Systematic Literature Review

A systematic literature review is according to Kitchenham (2004) a process that involves multiple activities, wherein it can be divided into three phases. Planning, conducting, and reporting. Further, these phases are broken into steps and are visualized in Figure 1. The methodology used in this work will be based upon the suggested process by Brereton et al. (2007) in Figure 1 and is visualized in Figure 2.

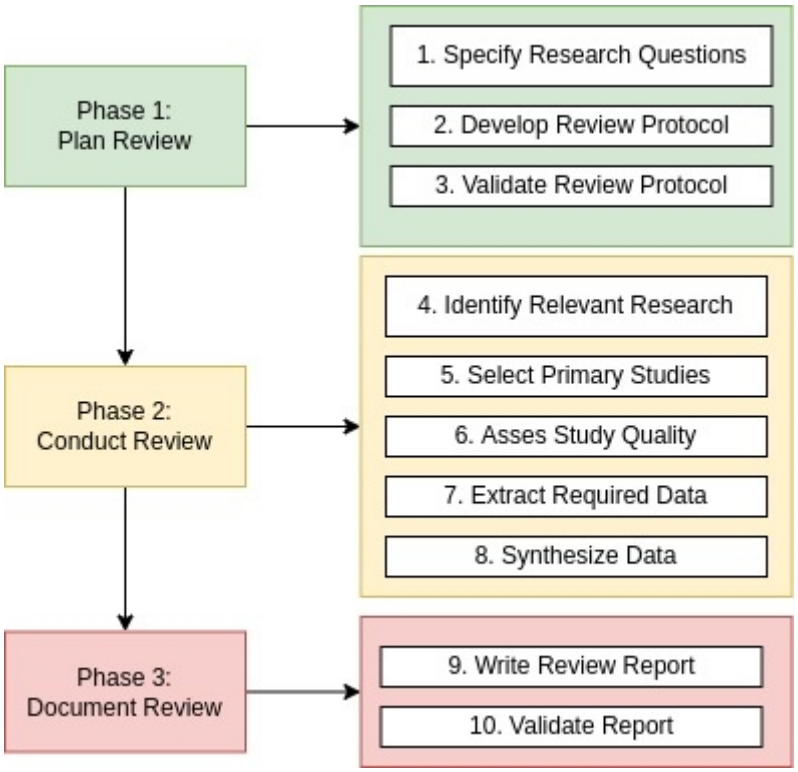

Figure 1: Systematic Literature Review process as described by Brereton et al. (2007) which is based on the phases proposed by Kitchenham (2004)

As seen in Figure 1 the work done during a structured literature review according to Brereton et al. (2007) begins with the definition of research questions that support the aim of the research and is according to Kitchenham (2004) the most important activity during the structured literature review work. The review protocol details the plan that is to be implemented in the work and contains the process, applicable conditions for the selection of studies, and quality metrics on selected articles, the protocol is also validated and reviewed by a third party (Brereton et al., 2007; Kitchenham, 2004). The process continues into the conduct phase where the strategies created in the protocol are executed and allow for the gathering of data by searching databases for relevant articles and selecting those that apply to the conditions set during the planning phase, these articles are then studied for quality, performing this process allows for a bibliography to be built that data can be extracted and synthesized from to answer the questions posed in the previous phase (Brereton et al., 2007). The process is finished

with documenting found results and formulating a conclusion based on them (Brereton et al., 2007).

Taking this process into consideration for this work a flow diagram was created to simplify the work that was to be done and allow the work to fit better into the authors' schedule, also to further give insight into how the work for this paper was done, see Figure 2. The first part of the Planning phase has been conducted and previously mentioned in Chapter 3.

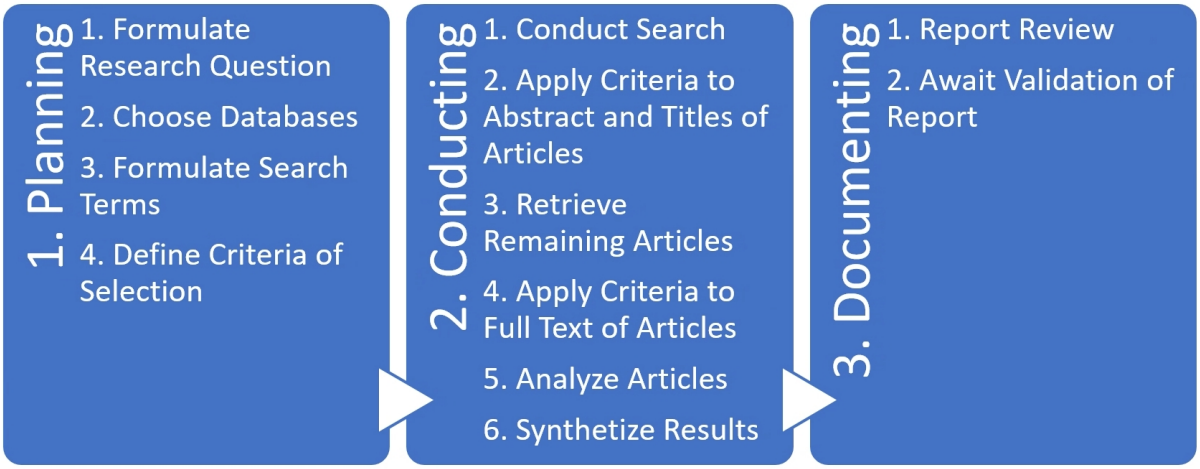

Figure 2: Workflow process created for, and applied, to this work

4.1.1 Databases

To gain a sufficient amount of data from the searches multiple databases have to be utilized, there exist a multitude of databases, however, some databases are more relevant than others, therefore certain limitations have to be set in which databases can be used. The first of these is the requirement that they are available through the University of Skövde's library and the second is that the database includes IT research papers. From the available databases, initially, three were chosen, ACM Digital Library, IEEE Xplore, and Web of Science. ACM and IEEE were chosen due to the abundance of literature that is published and stored in their databases as well as due to the known reputation of these databases, Scopus and Google Scholar were later added to ensure all relevant studies were found, bringing the total of selected databases to five. Web of Science and Scopus are reputable sources that collect articles from many different databases including ACM and IEEE, which should be of help to include any missed articles in the two databases. Lastly, Google Scholar was used to gather any remaining articles missed by the searches in the databases due to its wide search area.

Selected databases:

- ACM Digital Library
- IEEE Xplore

- Web of Science
- Scopus
- Google Scholar

4.1.2 Search Terms

To locate and build a bibliography the databases must be searched using a variety of search terms, which according to Kitchenham (2004) are derived from the research question. As previously mentioned the research question “How are cybersecurity training games utilized to increase cybersecurity awareness in individuals employed within organizations?” was formulated from the perceived research gap regarding cybersecurity training, from the research question a variety of terms can be derived, it should also be noted that before the research was done these keywords were tested against the databases in different combinations and showed promising results and they consist of the following:

- cybersecurity AND
    - corporations OR
    - organizations OR
    - business OR
    - professional OR
    - employee
- training AND
    - games OR
    - serious games

As stated these search terms were used in different combinations of AND and OR operands to include as many articles as possible in a single search, each search string has to be carefully crafted to properly work in each database as each is built differently and reads search strings in their unique way (Brereton et al., 2007).

4.1.3 Selection Criteria

In her paper, Kitchenham (2004) states that the selection criteria of studies should be decided during the planning phase and that the criteria should be based upon the research question and properly piloted to ensure that interpretation is always correct. As this study aims to find information regarding games as a tool to increase cybersecurity awareness it is important to exclude papers and articles that investigate areas of training outside of games. To properly assess studies these criteria should be listed in an organized manner to allow for the work to be conducted efficiently, see Table 1.

Inclusion Criteria	I1. Published in journal or conference
	I2. The article is written in English
	I3. Peer reviewed
	I4. Articles include research regarding games as a training tool to increase cybersecurity awareness of individuals in organizations
Exclusion Criteria	E1. Does not meet inclusion criteria
	E2. Payment required
	E3. Further login required
	E4. Duplicate of already collected article

Table 1: Inclusion and Exclusion Criteria

The inclusion criteria were chosen due to the impact they have upon articles as well as considerations for the actual implementation of the analysis of the work, most works today are written in English however there are always outliers, to make the work uniform however criteria I2 was created to ensure that all articles that pass the selection step are in English. Criteria I1 was implemented as journals and conference papers put a certain number of standards of quality in all papers published in them. The criteria I3 was chosen to allow for the articles to have a certain level of competency as they have cleared peer reviews and I4 was created to allow for a bibliography to be built that would be able to answer the research question. The exclusion criteria were chosen once the inclusion criteria had been set, E1 rejects any papers that do not meet the inclusion criteria whilst E2 and E3 reject papers that are not available for reading within the legal means of the author, which entails not being available for download through the resources available to the author and do not require payment or an additional login. E4 rejects all duplicates of articles that have already been included in the bibliography.

4.1.4 Backward Snowballing

Traditionally systematic literature reviews only search databases to build their bibliography, however, this can allow for certain articles to be missed in the analysis phase, to increase the area of search and allow for more articles to be found, that might be missed during the database searches the practice of backward snowballing can be applied by examining the reference list of all accepted articles (Kitchenham, 2004; Wohlin, 2014).

In this work backward snowballing will be applied to the accepted bibliography, wherein the referenced works will be analyzed starting at step 2, which applies the

inclusion and exclusion criteria on the abstract and title which is part of phase 2, the conducting phase, which can be seen in Figure 2. Due to the timeframe of the project, the backward snowballing will only be conducted once in each accepted article and any duplicates will be ignored completely, furthermore, the level of backward snowballing will only be applied to the articles that were accepted into the bibliography from the database searches, no backward snowballing will be applied to the articles accepted through the practice of backward snowballing.

4.1.5 Analysis method

There are two common methods of analysis utilized in systematic literature reviews, the two being grounded theory and thematic coding, also known as thematic analysis. This thesis paper will make use of thematic coding which according to Braun & Clarke (2006) starts with coding likened to open coding, where relevant text is marked and categorized into several categories that relate to the stated research question, and data is then extracted from categorized text to formulate the results, whilst their work focus on psychology they also state that the application of thematic coding is thoroughly utilized in many areas of research. The categories can be defined before the coding utilizing deductive reasoning or during the coding utilizing inductive reasoning, this study will utilize an inductive approach. Thematic coding is a flexible option when applying an analysis model and can therefore cover multiple angles during the analysis of qualitative data, wherein qualitative data involves a collection of data that defines a certain area of research (Braun & Clarke, 2006). In the process of thematic coding, it is the author that builds the formula of how the work of analysis is to be applied, including what themes should be looked for in the articles that are reviewed along with the categories (Braun & Clarke, 2006).

4.1.6 Validity

Through the implementation of a systematic literature review utilizing thematic coding multiple issues regarding its validity and trustworthiness can arise, it is therefore of great importance to address these issues and ensure that the study can meet the standards that are required of it. This subchapter will briefly discuss the validity and reliability of qualitative studies and how they can be threatened within the context of this study.

To ensure that validity and reliability standards are met within a qualitative work rigorous testing of the two has to be conducted, the method to assure validity and reliability is however not generally agreed upon wherein multiple researchers believe certain methods are superior to others, such as triangulation, realism, and constructivism (Golafshani, 2015). According to Golafshani (2015), validity and reliability in qualitative studies are conceptualized as trustworthiness, rigor, and quality, it is through this that bias in research articles can be eliminated and increase the

truthfulness of a researcher's proposition about a social phenomenon through different paradigms, which are suitable for different situations.

This article aims to uphold the validity and reliability through rigorous descriptions of each step in the processes performed to complete the study, by applying the literature search to two different databases known for works that specialize in IT subjects and three that collect articles from a large variety of sources, with a further application of backward snowballing all relevant articles are collected. With the correct application of the selection criteria in two steps, relevant articles are guaranteed to be included within the finalized bibliography.

Possible threats to validity and reliability are therefore rooted in the failure of finding all possible articles for the finished bibliography, doing thorough searches through multiple database sources is a necessity to combat this. Further threats to validity consist of failure to follow the methodology that is set within the paper before the search of databases along with the application of the selection criteria when selecting articles for the bibliography as well as improper analysis of the articles themselves.

5 Implementation of the methodology

This chapter describes and discusses how the methodology described in the previous chapter was implemented in the collection of articles for the accepted bibliography that will later be analyzed in the next chapter. The work done for this chapter starts in the conducting phase of the workflow to search the selected databases using the defined search strings from the previous chapter and applying the inclusion and exclusion criteria to the search results.

5.1 Article search result

The searched databases, along with search strings, the number of articles attained before selection criteria, and collected articles after the first and second selection criteria are presented in Table 2. The first selection applied the selection criteria to the title and abstract of the search results found within the databases and the second selection applied the criteria to the entirety of the selected articles from the first iteration. These iterations were applied to gather all relevant articles and discard all that was of no relevance to the topic.

Databases	Accessed	Results	1st Selection	2nd Selection	Search String
Web of Science	25-04-2022	55 Articles	24 Articles	6 Articles	ALL=((cybersecurity OR "cyber security") AND ("serious games" OR games) AND training AND (corporate OR corporation OR professional OR business OR enterprise OR employee OR organization))
IEEE Xplore	25-04-2022	33 Articles	8 Articles	1 Article	(cybersecurity OR "cyber security") AND ("serious games" OR games) AND training AND (corporate OR corporation OR professional OR business OR enterprise OR employee OR organization)
ACM Digital Library	25-04-2022	838 Articles	26 Articles	3 Articles	(cybersecurity OR "cyber security") AND ("serious games" OR games) AND (business OR employee OR professional OR corporate OR corporation OR enterprise OR organization) AND training
Scopus	25-04-2022	43 Articles	3 Articles	1 Article	TITLE-ABS-KEY((cybersecurity OR "cyber security") AND ("serious games" OR games) AND training AND (corporate OR corporation OR professional OR business OR enterprise OR employee OR organization)) AND (LIMIT-TO (SRCTYPE,"p") OR LIMIT-TO (SRCTYPE,"j")) AND (LIMIT-TO (DOCTYPE,"cp") OR LIMIT-TO (DOCTYPE,"ar"))
Google Scholar	27-04-2022	738 Articles	13 Articles	4 Articles	"serious game" cybersecurity "training" "organization"
Total Articles Before Backward Snowballing: 15					

Table 2: Performed searches, with remaining articles after selections

5.2 Backward Snowballing result

To allow for the further gathering of articles about the topic, the backward snowballing technique was applied to the articles that remained after the two selection stages. The articles have gone through both the first and second selection stages using the same criteria as stated in subchapter 4.1.3. The results of the backward snowballing technique can be seen in Table 3.

The number after 1st selection	The number after 2nd selection
37 Articles	6 Articles
Total Articles From Backward Snowballing: 6	
Total Articles After Backward Snowballing: 21	

Table 3: Results of backward snowballing

6 Analysis and results

After the extensive literature search was conducted, 21 papers were identified that discussed and researched games as a tool to increase cybersecurity awareness in individuals employed by organizations. All except one article were from 2016 or later which indicates a very young and developing field, the majority of which had positive results of utilizing games as a training tool to increase different aspects of cybersecurity of individuals in organizations and are mapped in Table 4. In this chapter the thematic coding described in the methodology chapter is applied to the collected bibliography of accepted articles, the articles' passages are examined for data regarding the search terms and are then further examined concerning the aims of the work and categorized into themes which were specified in subchapter 3.1. The articles are analyzed in themes regarding a general mapping of current games' design and what aspects of cybersecurity the different games teach to find out how they are utilized to increase cybersecurity awareness of individuals within organizations. The target audience and results of the studies will also be reported.

ID	Game Name	Description	Target Audience	Result	Study
A01	**GHOST**	A 3D simulation game within a spaceship environment has multiplayer	General Employees	Results of game training are positive. Participants' awareness is increased	(König & Wolf, 2018)
A02	**Cyber Shield Game**	Web-based challenge game	General employees	Cybersecurity awareness in employees raised by 50%	(Abu-Amara et al., 2021)
A03	**CySecEscape 2.0**	Virtual Escape room point and click adventure challenge game with 1-2 players	General employees	The game was positively received	(Löffler et al., 2021)
A04	**IoT-Poly**	Scenario card game with threats and countermeasures	Cybersecurity personnel	Positive player evaluation	(Omiya et al., 2019)
A05	**Operation Digital Chameleon**	Physical Red vs Blue team scenario simulation game, attackers vs defenders	IT personnel	The game improves players' process of finding means of attack and defense	(Rieb & Lechner, 2016)
A06	**Persuaded**	Digital Patience/Solitaire game. Attack cards and defense cards are used	General Employees	Players show increased knowledge regarding certain attacks	(Aladawy et al., 2018)
A07	**Phishy**	2D Fishing adventure challenge game	General Employees	Awareness of phishing is increased, less likely to be phished	(CJ et al., 2018)
A08	**Protect**	Online patience/solitaire game, based on Persuaded with enhanced configuration	General Employees	Positive results from participants	(Goeke et al., 2020)
A09	**Riskio**	Card game utilizing a game board, the game uses attack, defense, and info cards	General employees	Positive player feedback	(Hart et al., 2020)
A10	**SCIPS**	A digital scenario simulation game, players make cybersecurity decisions during events	Security professionals, managerial staff, IT employees Senior stakeholders	Risk identification skills and understanding of cybersecurity are increased Participant feedback is positive, the game meets the requirements, set to increase skills and knowledge	(O'Connor et al., 2021) (Cook et al., 2016)
A11	**Secu-One**	Card game, attack cards vs defense cards, discussion selects the best defense	Security personnel	Game results are positive and its effectiveness in raising motivation	(Omiya & Kadobayashi, 2019)
A12	**Decisions and Disruptions (D-D)**	Tabletop game with a game master, player team protects using set funds	Security experts, managers, and computer scientists	Participant feedback is positive regarding design and fun aspects, players found that knowledge of cybersecurity was increased	(Frey et al., 2019)
A13	**CSRAG**	Scenario roleplay card game	General Employees	Evaluation is indicated but not reported in the article itself	(Yasin et al., 2019)
A14	**N/A (Elicit social engineering requirements)**	Scenario card game, attack focused	IT employees, security engineers, IT admins, administration	Employees are most at risk of being targeted by attacks	(Beckers & Pape, 2016)

			staff		
A15	**CyberCIEGE**	Scenario simulation game, Sims style, the player acts as a security manager	IT personnel	Evaluation is indicated but not reported in the article itself	(Cone et al., 2007)
A16	**HackLearn**	Hacking simulation game	Computer professionals with a cybersecurity background	Results evaluate game positively as a training medium	(Katsantonis et al., 2021)
A17	**Passworld**	2D adventure challenge platform game	General Employees	Players showed improvements in creating unique passwords	(Jayakrishnan et al., 2020)
A18	**HATCH**	A card Game, behavior cards are exploited by attack cards, players attack from inside or outside.	General Employees	Players were able to elicit threats to situations in the game	(Beckers et al., 2016)
A19	**InfoSecure**	Web-based hospital simulation game	General employees	The game was effective as a training medium	(Ghazvini & Shukur, 2018)
A20	**GAP**	2D Maze adventure puzzle game	General Employees	Participants could identify insecure password practices better	(Tupsamudre et al., 2018)

Table 4: Mapping of Games, with results and target audience

6.1 Design

Games are designed within different mediums and to understand how games are utilized to increase the cybersecurity knowledge of employees, the mediums the games use to disseminate their information to the players must be analyzed. The games were mapped into three distinct categories through analysis of the articles utilizing the inductive thematic analysis to find common themes within the games, based on the medium and design of the games, the most populous of them being card & board games (10 games), challenge games (5 games) and simulation games (6 articles, 5 games) see Table 5. The following subchapters describe and map the games in further detail.

Design	Description	Games
Card and Board Games	The game consists of cards or a game board, digital and non-digital	A04, A05, A06, A08, A09, A11, A12, A13, A14, A18
Challenge Games	The game consists of challenges and puzzles	A02, A03, A07, A17, A20
Simulation Games	The game consists of performing tasks and objectives similar to a real-world setting	A01, A10, A15, A16, A19

Table 5: Mapping of Game Design

6.1.1 Card & Board Games

Card games, as well as board games, have long since been a staple in entertainment, and from the analysis of the articles, it can be seen that they also work well within a cybersecurity educational context. The researchers have within these articles studied games that focus on reacting to threats with defense cards in different scenarios and most of which with an aspect of teamwork, this immediate on-the-spot attack and defense game-play and teamwork allows for open discussion about the topics taught which the researchers report increases the subjects' confidence and knowledge of cybersecurity, with a surprisingly diverse targeted audience of the games. Most of the researched games are physical tabletop (8 games) with the remaining being digital (2 games), the games show positive results both qualitative and quantitative except for A13 which indicates evaluation has taken place but is not reported.

Among the card & board games only A06, and A08 were single-player focused, with A08 employing further scenarios and further configurations of difficulty and challenges. The games are similar to the traditional card game solitaire but use information cards consisting of attack cards and response cards, in the form of specific or wildcard defenses optionally skip round cards. The games employ a "see the future" mechanism which allows for the player to think ahead and can therefore plan accordingly. This allows the game-play to teach its audience on the spot regarding the attacks that are presented as they have to respond with a defense, or another action, if not they lose.

War-gaming paradigms are used in A05 to create an attack and defense simulation game with discussion elements allowing for deeper participant learning. A14 and A18 utilize a traditional tabletop experience to launch attacks and discuss the feasibility of said attack, which allows for a deeper understanding of the if and how threats can exploit vulnerabilities. A11 utilizes similar mechanisms but has security personnel responding to a singular attack with defenses that are required to be explained why they are most suited, followed by discussion. The physical tabletop games' focus on social interactions and team-building through discussion-based learning utilizing information cards is highlighted in A09 which follows a similar game loop to A11 but includes the aspect of a game master describing a scenario where the attack is plausible and how it may be realized. In A09 the attacking player is rotated to give all participants an attacker and defender perspective. With the description given during the presentation of attack cards and defense response with arguments for why the suggested defense is the most suitable, and the game master leading the discussion. This exemplifies the discussion-based learning seen in most card & board games, allowing for training through team-based efforts which improve team cohesiveness and combined awareness of cybersecurity.

Along this line of mechanisms A04 similarly utilizes heavy discussion-based learning in cybersecurity personnel through setting up IoT environments, their attack surfaces, threats, and countermeasures. A role-playing element is introduced in A12 and A13 and is especially highlighted with discussion-based learning in A12 which utilizes a single team-based security personnel perspective with players against a game master to build defenses using a set budget against a wide variety of attacks, created by the game master, to allow for greater understanding of threat scenarios. Defenses are freely invested in by the players through discussion within the team, allowing for the player team to understand each scenario and how in future rounds different defenses might be more effective. Similar mechanisms are utilized in A13 which focuses the learning process on an attacker's perspective to give insight into the processes of threats being realized.

6.1.2 Challenge Games

The researchers have within these articles studied digital games that focus on linear game-play that puts the player(s) through a series of cybersecurity challenges and puzzles to increase knowledge of different aspects surrounding cybersecurity. The researchers in each article present a game that consists of different game-play loops which shows the versatility that can be achieved when utilizing digital games. The games presented all have a similar wide targeted audience of being aimed at the general employee population within organizations, as these types of games have a friendly exterior and require little gaming knowledge to play, and are easy to distribute, and the research indicates positive results, with all except A02 being quantitative. The researched games are all single-player experiences, with A03 reportedly allowing for a second player to encourage discussion during game-play.

These researched games have a further common theme of educating in shorter bursts during the game-play, with feedback and results being given after either each level or game-play round. This is exemplified in A02 which raises awareness in the players through a series of interactive quiz-style puzzles and challenges in an office environment utilizing several levels regarding different cybersecurity topics. This environment allows the players to understand the impact that threats can have when realized in the real-world counterpart. This is further seen in A07, A17, and A20 which utilize scenario-based level design to educate players, and for the players to understand each situation and formulate a plan to react accordingly. A03, A07, and A20 further these scenarios with a larger focus on visual game-play of the training to enhance it and increase user retention during the sessions. Education during game-play is highlighted in A03 which utilizes a virtual escape room in a small to medium-size enterprise environment to investigate cybercrime and find a rogue employee. The players further the games' progression by completing cybersecurity puzzles, allowing players to understand how a lack of certain security practices can impact cybersecurity.

This trend continues with A07, A17, and A20 applying real-time action to give players a sense of excitement and urgency to complete their tasks. This is especially highlighted in A07 through the use of a fishing environment with a visualized danger (tiger), wherein the player has to reach the shore by completing a set of challenges over multiple levels consisting of hooking fish, answering phishing-related questions, and avoiding dangerous aquatic wildlife. The game is progressed through successful completion of these challenges, with subsequent failures causing the danger of becoming closer to being realized, which raises awareness of how improper scrutiny of mail can lead to devastating results.

6.1.3 Simulation Games

In the analyzed research simulation games put the player(s) in different simulated situations where daily tasks are simulated and evaluated concerning how well the task is performed and cybersecurity. The games have further shown to have a targeted audience that focuses on more advanced users while A01 and A19 have a broader targeted audience within organizations. The researchers show that putting players into simulated realities that allow them to fail or succeed without real consequences gives them an edge in understanding cybersecurity and the threats that are posed to it. As results of playing the games are positive in all cases except for A15 where it is implied that evaluation took place but was not reported within the article.

Among the simulations analyzed and collected for this study A01 and A15 utilize a 3D play area to simulate a workspace, with tasks to educate the players. The play area is further developed in A01 to include a futuristic spaceship command center to increase player retention during sessions and can further discussion through multiplayer capabilities. A01 employs these aspects to allow for control of a player character in a tablet and turn-based game, where players can experience interactions with cybersecurity, which includes defenses, threats, and vulnerabilities. In A01 players are tasked with performing quests that simulate real-life work tasks that can be completed through multiple choices, with certain choices having a better outcome, which the player is informed of at the end of the quest. An attack and defense simulation setting with discussion and budget management elements is highlighted in A10 allowing for deeper participant learning. The setting employed within A10 creates a simulated team-based environment that aims to raise awareness of cybersecurity through informed decisions within certain events of a scenario concluding with session feedback. The members of the teams are assigned roles that are required to perform different tasks and create defense strategies in the form of cards against perceived attacks to maintain the CIA of the simulated organization within the scenario. A16 employs a digital scenario hacking simulation that utilizes penetration tools to educate the players from an attack perspective regarding technical defenses and threats, through the player conducting penetration tests to find vulnerabilities in the targeted systems. A19

employs a casual game approach within a simulation context, with a workplace or attacker perspective to educate participants regarding threats and threat sources.

6.2 Teaching Aim

To further understand how games are utilized to increase cybersecurity awareness of individuals in organizations, analyzing which aspects of cybersecurity the games aim to teach to their players is therefore necessary. These aims have been categorized into three categories through thematic analysis of the selected bibliography, by analyzing the studies for teaching aims that relate to cybersecurity threats and defenses a finished mapping could be complete as seen in Table 6.

Card & board games are used to teach about the technical and social engineering aspect of cybersecurity, the reaction based game-play found in the games regarding threats and defenses allow for participants to calmly evaluate a wide range of attacks and perform countermeasures to show their understanding of how the social or technical threat works and how it can affect them. The challenge-based games are used to teach about the password and social engineering aspects, the challenge and puzzle settings increase the level of experimentation that the player can implement to find the best suitable options for each challenge or puzzle, which when targeting password practices and social-based attacks allows for increased understanding through repetition. The simulation games teach mostly regarding the overarching aspects of cybersecurity, their simulated nature allows multiple aspects to be investigated at the same time through the assuming of a role, performing regular tasks, and whilst discovering and defending against threats. The simulation games teach mostly regarding the overarching aspects of cybersecurity, their simulated nature allows for investigation of multiple aspects at the same time through the assuming of a role, performing regular tasks, whilst discovering and defending against threats. Except for A16 which strictly focuses on technical security from a hacking perspective and A10 from a defense perspective.

The technical knowledge category is the most plentiful taught area of cybersecurity (11 games) showing the importance of training the aspect as its main target audience are computer professionals, with social engineering knowledge (10 games) being a common theme amongst all types of design, showing its prevalence and importance in cybersecurity and password knowledge category (7 games) being the least taught area targeting general staff with a smaller amount of knowledge surrounding cybersecurity.

Aim / Game	Social Engineering Knowledge	Password Knowledge	Technical Knowledge
Card & Board Games	A06, A08, A12, A13, A18		A04, A05, A09, A11, A12, A13
Challenge Games	A02, A07	A02, A03, A17, A20	
Simulation Games	A01, A15, A19	A01, A15, A19	A01, A10, A15, A16, A19

Table 6: Mapping of Design cross-analyzed with the aspects of cybersecurity taught

6.2.1 Social Engineering Knowledge

The social engineering category involves threats that directly target humans and aims to increase the knowledge of the participants regarding social engineering attacks and allow for a greater understanding of how to protect themselves and systems against social engineering threats. The challenge-based games focus on a smaller range of social engineering topics, exemplified in A07 wherein phishing attacks are highlighted and aim to train users in identifying phishing URLs, familiarize the users with shortened URLs, and teach them how to find legitimate brand names in online searches. Similarly, the simulation games highlight certain topics through tasks, exhibited in A19, that delve into the topics of phishing and prominent strategies such as shoulder surfing, to protect information when utilizing a workstation. Further topics are raised in A01, where road apples and phishing threats are displayed to inform the players regarding the strategies that should be employed to mitigate or eliminate the threats and the consequences if realized. The card and board games broach the topic from a wider perspective of social engineering by delving into threat scenarios which are demonstrated in A18. The game aims to give players overarching knowledge of how social engineering attacks can be realized through vulnerabilities in human behavior, which allows for the players to understand how to protect themselves and the computer systems that exist against malicious actors.

6.2.2 Password Knowledge

The password category aims to impart knowledge regarding password creation and storage strategies as well as an understanding of the consequences surrounding vulnerabilities of weak passwords to the participants to secure workstations and systems from malicious actors. Password creation strategies and the knowledge of the complexity of passwords are highlighted in A17 where players are informed of password heuristics throughout the game and challenged to create strong passwords to protect themselves and collected artifacts. The training of creating strong and memorable passwords is presented as a task in A01 to increase knowledge regarding the building blocks of secure and well-made passwords. Poor password strategies are highlighted in A20 to raise awareness of the consequences of their utilization through

challenges that are overcome by game mechanisms similar to brute force password cracking.

6.2.3 Technical Knowledge

The Technical category involves threats that target systems and aims to train participants in understanding cyber threats, including their sources, mechanisms, and how they are realized. It also aims to give a general or in-depth understanding of the technical protection systems, including the building blocks of the systems and how to correctly build and configure them. Knowledge of penetration tools, cyber threats, and vulnerabilities is highlighted in A16 to raise awareness of the players regarding how these tools are utilized and what vulnerabilities are exploited in successful attacks. Training in cyber-attack methods and the Cyber Kill Chain are highlighted in A11 to allow players to understand the underlying technical protections that can be applied and the vulnerabilities that the attacks can exploit. Defensive strategies against various cyber threats are highlighted in A12 to broaden the players' understanding of attacks and the interactions different defenses have with threats.

7 Conclusion

By systematically analyzing 21 peer-reviewed articles that research the design of serious games, which aim is to raise cybersecurity awareness in organizational environments and the aspects of cybersecurity trained, show a young and promising field of research.

The articles mostly report positive results of the games as a training method within organizations to increase players' knowledge and awareness of cybersecurity-related subjects, however, some articles indicate evaluations, with failure to report within the study. Through the analysis applied it's shown how serious games utilize similar techniques and strategies to educate their targeted audience, these were mapped into three distinct categories regarding design mediums, consisting of card & board games, challenge games, and simulation games. Further when cross-analyzed with the categorized cybersecurity subjects trained, consisting of social engineering knowledge, password knowledge, and technical knowledge, it's indicated that games utilizing certain techniques are more likely to teach about certain topics with a favored targeted audience, which allows for the conclusion to be drawn of how games are implemented within organizations to increase cybersecurity awareness.

The card & board games utilized strategies of reactionary learning with discussion elements to increase technical and social engineering knowledge. The challenge games utilized linear game-play strategies of challenges and puzzles with changes in topics or furthering difficulty in short bursts and immediate feedback to increase social engineering and password knowledge. The simulation games utilized strategies of immersion-based learning to increase the broader knowledge of cybersecurity. To better understand the connections between design medium and trained aspects, further research could address this by delving deeper into the psychology and reasoning behind certain game-design strategies used to teach different aspects of cybersecurity, to find optimal ways of education using game-based learning.

This study contributes to the field of cybersecurity training and game-based learning within an organizational context, by reviewing and analyzing articles researching games as a cybersecurity training tool, an overview is formed regarding how training games are deployed and what their purpose of training is. The benefit that this article brings, regards IT professionals and researchers alike, the established overview allows both groups to understand how the games are created and deployed, with IT professionals being able to make informed decisions if they are to implement cybersecurity training within their organization. This also extends to researchers as it would be able to act as a basis for further research within the game-based learning of cybersecurity, and could allow for gaps to be found regarding how games are currently utilized within a cybersecurity context, as this thesis has mapped and discussed the

current landscape which shows what exists and what is being taught allowing for the possibility of designing new games to train cybersecurity.

8 Discussion

This chapter will contemplate the entirety of the systematic literature review performed, from the methodology's planning and arguments to its implementation, with the weaknesses and strengths being discussed in-depth, and results regarding the topic of this study. This chapter further delves into the ethical implication of the work, as well as a brief discussion regarding contributions to the field and how it can affect future research or implementations of a similar nature to the studied topic of this work, and how possible angles of research regarding the topic can be approached to strengthen the cumulative knowledge regarding games as a cybersecurity training tools within organizational contexts.

8.1 Implementation of Review

A qualitative systematic literature review utilizing a thematic analysis was the chosen methodology of this work as it allowed for the maximum amount of information gathering in the smallest amount of time, which was needed due to the strict time frame of this project. The study has followed the defined methodology in chapter 4, to ensure that the work is academically valid throughout the entirety of the study. Due to the nature of the study, only academic works published in journals and conferences have been collected and analyzed, this limitation potentially misses any commercially made game or in-house developed game by organizations, an interview-based study would allow for the gathering of similar information from researchers, developers and organizations to create a larger field of study. The study could further be strengthened through a product search outside of academic literature as a supplementary source of information and increase the value of the found results.

The databases selected were increased to include Scopus and Google Scholar after the collection of the articles for the bibliography to ensure that all relevant articles to the area of study were included and that the validity of the research wouldn't be threatened. The selection of further database searches would prove to be beneficial to the study as an increased amount of articles for the bibliography were found, the narrow focus of this study and the youthfulness of the research area resulted in a relatively small but still stable bibliography.

The use of further keywords could increase the number of relevant articles, or the ones implemented could be used more smartly as a larger amount of OR operands were used to widen the scope as much as possible during each search. Another issue that arose during the database searches which increased the number of search results, was the fact that searches in the databases except for Scopus included the text within the articles, which lead to irrelevant results however this can be justified as it allows for completeness in the search.

Encountered difficulties during the analysis of the collected bibliography were the documented results and implications of the authors' implementations in their research. A large portion of the studies do not discuss any long-term benefits of their implementations in regards to game-based learning as a training medium, how they are advantageous to other implementations, why they utilized certain game design aspects within their implementations, and if those aspects have an impact on the cybersecurity subjects taught through the game-play. Which limited the analysis and a forced focus on design implementations and cybersecurity subject and their correlation.

The results from this systematic literature review display that implementations that follow distinct strategies in the dissemination of information favor teaching certain cybersecurity topics, with different targeted audiences being favored depending on the topic. A larger amount of articles than expected detailed games that focused on teaching technical cybersecurity knowledge to IT professionals, rather than the broader less technologically knowledgeable employees, according to Chowdhury & Gkioulos (2021a) most threats that are realized come in the form of social engineering and exploit humans directly.

8.2 Ethical and societal aspects

Games can teach a multitude of subjects from many angles, certain games are targeted towards IT professionals and are utilized to train from a malicious actor perspective and can give insight into penetration testing which could then be utilized for malicious purposes or to better understand how sensitive information should be protected. Games can teach IT professionals about ethical dilemmas that might arise during their work, as sensitive information is transmitted and stored within their areas of operation. By being taught through games, IT professionals can be prepared on how they should interact with the sensitive information that they might face during their work tasks.

Through this study, the result of how games are applied and who and what they teach is presented and discussed which allows for the understanding of what areas of cybersecurity are trained. From this what is not being trained can be obtained, this knowledge can be maliciously exploited as it can allow for specific attack vectors to be formed. However, the impacts of this are dubious as game-based learning is only one of the methods to increase cybersecurity awareness in organizations. The societal aspects of this work are greater, however, as the mapping and explanation of how the games are utilized, gives researchers, developers, and professionals alike an overview of current existing implementations and can aid in the future work of new implementations or improvements upon existing ones, which can lead to better and more optimal methods of increasing cybersecurity awareness in organizations or education.

8.3 Contribution

This work fills the gap that currently exists within systematic literature reviews regarding games as a training method to teach cybersecurity within organizations through the analysis of available articles. Similar works exist but focus on a wider audience of school-age individuals and the general population with a variety of training methods which includes games. The results of game-based training have been reported briefly within this thesis and show that games can positively increase cybersecurity awareness within organizational contexts, which correlates with the results reported by Aldawood and Skinner (2018) as well as Chowdhury and Gkioulos (2021a) regarding games as a training medium and their effect on engagement levels.

As detailed in the thesis through the categorization of card and board games, it is shown that their design differs from the games used in non-organizational environments which as reported in research by Quayyum et al. (2021) have been mostly digital and utilized single-player experiences, that are similar to the challenge games categorized within this work. This thesis further contributes by reporting the differences that are present within the design choices of game medium and information dissemination within an organizational context, which gives a deeper understanding of how the games are utilized compared with the research done by Hendrix et al. (2016) which tried to understand the suitability of games as a cybersecurity training tool.

8.4 Future Work

Future research on the topic of games as a cybersecurity training tool could delve deeper into the subject presented in this work by utilizing an interview-based methodology to find further games and gain a deeper understanding of researchers, and developers' thoughts, motives, and reasoning behind their selected implementations for cybersecurity awareness in organizations, and through interviews with organizations that have applied games as a training tool could find additional games and their impacts both short term and long term.

Further research could also investigate the link between the medium of the game and the cybersecurity subjects that are taught, a case study could be utilized to test and evaluate different game mediums and their effectiveness in teaching specific cybersecurity subjects, depending on the result of this type of work it could then be utilized in future game-based learning implementations.

9 References

Abu-Amara, F., Almansoori, R., Alharbi, S., Alharbi, M., & Alshehhi, A. (2021). A novel SETA-based gamification framework to raise cybersecurity awareness. *International Journal of Information Technology*, *13*(6), 2371–2380. https://doi.org/10.1007/s41870-021-00760-5

Aciego, R., García, L., & Betancort, M. (2012). The Benefits of Chess for the Intellectual and Social-Emotional Enrichment in Schoolchildren. *The Spanish Journal of Psychology*, *15*(2), 551–559. https://doi.org/10.5209/rev_sjop.2012.v15.n2.38866

Aladawy, D., Beckers, K., & Pape, S. (2018). PERSUADED: Fighting Social Engineering Attacks with a Serious Game. *Trust, Privacy, and Security in Digital Business*, 103–118. https://doi.org/10.1007/978-3-319-98385-1_8

Al-Azawi, R., Al-Faliti, F., & Al-Blushi, M. (2016). Educational Gamification Vs. Game Based Learning: Comparative Study. *International Journal of Innovation, Management and Technology*, 131–136. https://doi.org/10.18178/ijimt.2016.7.4.659

Aldawood, H., & Skinner, G. (2018). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*. https://doi.org/10.1109/tale.2018.8615162

Beckers, K., & Pape, S. (2016). A Serious Game for Eliciting Social Engineering Security Requirements. *2016 IEEE 24th International Requirements Engineering Conference (RE)*. https://doi.org/10.1109/re.2016.39

Beckers, K., Pape, S., & Fries, V. (2016). HATCH: Hack And Trick Capricious Humans – A Serious Game on Social Engineering. *Electronic Workshops in Computing*. https://doi.org/10.14236/ewic/hci2016.94

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systems and Software*, *80*(4), 571–583. https://doi.org/10.1016/j.jss.2006.07.009

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. *Journal of Experimental Criminology*, *11*(1), 97–115. https://doi.org/10.1007/s11292-014-9222-7

Carl, G., Kesidis, G., Brooks, R., & Suresh Rai. (2006). Denial-of-service attack-detection techniques. IEEE Internet Computing, 10(1), 82–89. https://doi.org/10.1109/mic.2006.5

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, *106*, 1–20. https://doi.org/10.1016/j.eswa.2018.03.050

Chowdhury, N., & Gkioulos, V. (2021a). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, *40*, 100361. https://doi.org/10.1016/j.cosrev.2021.100361

Chowdhury, N., & Gkioulos, V. (2021b). Key competencies for critical infrastructure cyber-security: a systematic literature review. *Information & Computer Security*, *29*(5), 697–723. https://doi.org/10.1108/ics-07-2020-0121

CJ, G., Pandit, S., Vaddepalli, S., Tupsamudre, H., Banahatti, V., & Lodha, S. (2018). PHISHY - A Serious Game to Train Enterprise Users on Phishing Awareness. *Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts*. https://doi.org/10.1145/3270316.3273042

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security*, *26*(1), 63–72. https://doi.org/10.1016/j.cose.2006.10.005

Cook, A. F., Smith, R., Maglaras, L. A., & Janicke, H. (2016). Using Gamification to Raise Awareness of Cyber Threats to Critical National Infrastructure. *Electronic Workshops in Computing*. https://doi.org/10.14236/ewic/ics2016.10

Djaouti, D., Alvarez, J., Jessel, J. P., & Rampnoux, O. (2011). Origins of Serious Games. *Serious Games and Edutainment Applications*, 25–43. https://doi.org/10.1007/978-1-4471-2161-9_3

Fergus, S., & Zimmerman, M. A. (2005). ADOLESCENT RESILIENCE: A Framework for Understanding Healthy Development in the Face of Risk. *Annual Review of Public Health*, *26*(1), 399–419. https://doi.org/10.1146/annurev.publhealth.26.021304.144357

Frey, S., Rashid, A., Anthonysamy, P., Pinto-Albuquerque, M., & Naqvi, S. A. (2019). The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game. *IEEE Transactions on Software Engineering*, *45*(5), 521–536. https://doi.org/10.1109/tse.2017.2782813

Ghafir, I., Prenosil, V., Svoboda, J., & Hammoudeh, M. (2016). A Survey on Network Security Monitoring Systems. *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*. https://doi.org/10.1109/w-ficloud.2016.30

Ghazvini, A., & Shukur, Z. (2018). A Serious Game for Healthcare Industry: Information Security Awareness Training Program for Hospital Universiti Kebangsaan Malaysia. *International Journal of Advanced Computer Science and Applications*, *9*(9). https://doi.org/10.14569/ijacsa.2018.090932

Goeke, L., Quintanar, A., Beckers, K., & Pape, S. (2020). PROTECT – An Easy Configurable Serious Game to Train Employees Against Social Engineering Attacks. *Computer Security*, 156–171. https://doi.org/10.1007/978-3-030-42051-2_11

Golafshani, N. (2015). Understanding Reliability and Validity in Qualitative Research. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2003.1870

Graafland, M., Schraagen, J. M., & Schijven, M. P. (2012). Systematic review of serious games for medical education and surgical skills training. *British Journal of Surgery*, *99*(10), 1322–1330. https://doi.org/10.1002/bjs.8819

Gundu, T. (2019). Acknowledging and Reducing the Knowing and Doing Gap in Employee Cybersecurity Compliance. *ICCWS 2019 14th International Conference on Cyber Warfare and Security*, 94–102.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security*, *95*, 101827. https://doi.org/10.1016/j.cose.2020.101827

Hendrix, M., Al-Sherbaz, A., & Bloom, V. (2016). Game Based Cyber Security Training: are Serious Games suitable for cyber security training? *International Journal of Serious Games*, *3*(1). https://doi.org/10.17083/ijsg.v3i1.107

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology*, *32*(6), 584–593. https://doi.org/10.1080/0144929x.2011.632650

Jayakrishnan, G. C., Sirigireddy, G. R., Vaddepalli, S., Banahatti, V., Lohda, S. P., & Pandit, S. S. (2020). Passworld: a serious game to promote password awareness and diversity in an enterprise. *SOUPS'20: Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security*, 1–18.

Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018). Evaluation of Game-Based Learning in Cybersecurity Education for High School Students. *Journal of Education and Learning (EduLearn)*, *12*(1), 150–158. https://doi.org/10.11591/edulearn.v12i1.7736

Katsantonis, M. N., Mavridis, I., & Gritzalis, D. (2021). Design and Evaluation of COFELET-based Approaches for Cyber Security Learning and Training. *Computers & Security*, *105*, 102263. https://doi.org/10.1016/j.cose.2021.102263

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

Kim, S. H., Wang, Q. H., & Ullrich, J. B. (2012). A comparative study of cyberattacks. *Communications of the ACM*, *55*(3), 66–73. https://doi.org/10.1145/2093548.2093568

Kitchenham, B. (2004, July). *Procedures for Performing Systematic Reviews*. https://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf

König, J. A., & Wolf, M. R. (2018). GHOST: An Evaluated Competence Developing Game. *International Journal on Advances in Security*, *11*(3 & 4), 274–287.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

Löffler, E., Schneider, B., Zanwar, T., & Asprion, P. M. (2021). CySecEscape 2.0—A Virtual Escape Room To Raise Cybersecurity Awareness. *International Journal of Serious Games*, *8*(1), 59–70. https://doi.org/10.17083/ijsg.v8i1.413

Mallik, A. (2019). MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS. Cyberspace: Jurnal Pendidikan Teknologi Informasi, 2(2), 109. https://doi.org/10.22373/cj.v2i2.3453

O'Connor, S., Hasshu, S., Bielby, J., Colreavy-Donnelly, S., Kuhn, S., Caraffini, F., & Smith, R. (2021). SCIPS: A serious game using a guidance mechanic to scaffold effective training for cyber security. *Information Sciences*, *580*, 524–540. https://doi.org/10.1016/j.ins.2021.08.098

Okoli, C., & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1954824

Omiya, T., Fall, D., & Kadobayashi, Y. (2019). IoT-Poly. *Proceedings of the 19th Koli Calling International Conference on Computing Education Research*. https://doi.org/10.1145/3364510.3364519

Omiya, T., & Kadobayashi, Y. (2019). Secu-One. *Proceedings of the 2019 7th International Conference on Information and Education Technology - ICIET 2019*. https://doi.org/10.1145/3323771.3323792

Plass, J. L., Homer, B. D., & Kinzer, C. K. (2015). Foundations of Game-Based Learning. *Educational Psychologist*, *50*(4), 258–283. https://doi.org/10.1080/00461520.2015.1122533

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, *30*, 100343. https://doi.org/10.1016/j.ijcci.2021.100343

Razak, M. F. A., Anuar, N. B., Salleh, R., & Firdaus, A. (2016). The rise of "malware": Bibliometric analysis of malware study. Journal of Network and Computer Applications, 75, 58–76. https://doi.org/10.1016/j.jnca.2016.08.022

Rieb, A., & Lechner, U. (2016). Operation Digital Chameleon. *Proceedings of the 12th International Symposium on Open Collaboration*. https://doi.org/10.1145/2957792.2957800

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Santos, R. E., & Silva, F. Q. D. (2013). Motivation to Perform Systematic Reviews and their Impact on Software Engineering Practice. *2013 ACM / IEEE International Symposium*

on Empirical Software Engineering and Measurement. https://doi.org/10.1109/esem.2013.36

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-Phishing Phil. *Proceedings of the 3rd Symposium on Usable Privacy and Security - SOUPS '07*. https://doi.org/10.1145/1280680.1280692

Skarga-Bandurova, I., Ryazantsev, A., & Kiryushatova, K. (2016). An Experience Report on Education and Training Programme in Cybersecurity of Critical Infrastructures. *Information & Security: An International Journal*, *35*, 123–132. https://doi.org/10.11610/isij.3506

Smith, A., Papadaki, M., & Furnell, S. M. (2013). Improving Awareness of Social Engineering Attacks. *Information Assurance and Security Education and Training*, 249–256. https://doi.org/10.1007/978-3-642-39377-8_29

Tupsamudre, H., Wasnik, R., Biswas, S., Pandit, S., Vaddepalli, S., Shinde, A., Gokul, C. J., Banahatti, V., & Lodha, S. (2018). GAP: A Game for Improving Awareness About Passwords. *Serious Games*, 66–78. https://doi.org/10.1007/978-3-030-02762-9_8

Weber, K., Schütz, A. E., Fertig, T., & Müller, N. H. (2020). Exploiting the Human Factor: Social Engineering Attacks on Cryptocurrency Users. *Learning and Collaboration Technologies. Human and Technology Ecosystems*, 650–668. https://doi.org/10.1007/978-3-030-50506-6_45

Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering - EASE '14*. https://doi.org/10.1145/2601248.2601268

Yasin, A., Liu, L., Li, T., Fatima, R., & Jianmin, W. (2019). Improving software security awareness using a serious game. *IET Software*, *13*(2), 159–169. https://doi.org/10.1049/iet-sen.2018.5095

Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4), 297–307.

Zhonggen, Y. (2019). A Meta-Analysis of Use of Serious Games in Education over a Decade. *International Journal of Computer Games Technology*, *2019*, 1–8. https://doi.org/10.1155/2019/4797032