CyberSecurity and gamification of cybersecurity training

Andrej Jerman Blažič
Laboratory for open system and networks, Institute Jožef Stefan, Ljubljana, Slovenia
Fall 2021

Abstract

Cyber security is one of the most important technological and political subject in the world today, due to almost continuous revelations of incidents and breaches and the economic damage to many intuitions, states and users of electronic communications. In this context of unpredictability and insecurity on the networks, organizations are redefining their approach to cyber security, trying to find the balance between risk, innovation and cost of protection. At the same time, the field of cyber security is undergoing many dramatic changes, demanding organizations embrace new practices and skill sets that are needed to be acquired by their employees.. With recent high-profile attacks it has become clear that training in cyber security is needed almost in any intuition or organization. Cybersecurity education is today new field of application were new educational approaches are applied among them serious games that enable better skill training. Serious Games have the capability to be effective tools for public engagement and behavioural change and role play games, are already used by security professionals engaged in skill training and education. The cyber security education seems especially well-suited for use of Serious Games that enable interactivity in the training and the acquiring of skills. This report in the first part presents the effective cyber security educational tools such are CyberSecurity games and in second part it presents the evaluation of the selected CyberSecurity games, that have been selected as best tools in cybersecurity training by world wide web literature reviews.

1. Introduction

Would you be comfortable living in a house that someone else had the key to? What if an underground tunnel led into it from a public park, or its windows could never quite close all the way? Would you trust it with your safety and your privacy? The internet is that house. This is not to say—never go into the house, but rather, you should know the hazards before you store all of your valuable content there—and do what you can to protect them.

So why is internet insecure, and why it can't be sufficiently fortified to be safe?

Since the introduction of the Internet and the related application, back in history, this network was not originally built to be what it is today. The internet originally has been developed when computers (a.k.a. supercomputers) were in the size of the big closet and they were owned only by universities, academic institutions, big businesses companies, military institutions and a few governments. The point, originally, was to let these massive supercomputers to be connected for exchange of data. Internet was developed for communicating orders and data in case of war as in its beginning it was project of USA DARPA agency. As soon as three computers from different providers with different operating systems could exchange information between them, the network was created. The network gradually grew, until personal computers (PC) emerged in the 1980s, and then the growth of internet connected PCs rapidly expanded. The consumption of the PC market was rising and the PCs were in presence in every household.

Soon people were not just talking to each other and exchanging data over the network, but also they started to exchange money, play games, reading on-line news, shopping, planning their daily schedule and holidays, publishing photos, music, videos, working from home and doing everything what we associate with the internet today. Other ICT devices started talking to the network too, by sending an email, making a bank transfer, ordering something online or booking their flights directly from mobile phones. The lifestyle has never been as easy and fast as today. About 50 billion devices is the estimate to be connected to the Internet up to 2020, most of them are barely protected, a fact that implies as many potential doors for hackers to intrude in the connected devices, companies, homes and personal lives.

The ease of communicating each of these devices to others via the network came at a high price: security and safety was forgotten. In the simple way-for example: one computer can send instructions for deleting the crucial data and reshaping them for blackmailing — in another term. Some of these technics known as undesired guests are viruses and malware. Furthermore, one person could steal another's identity by cracking, or extracting a password in the owner device.

The current connectivity of the network enable various organizations to become more business efficient, more productive and better informed. Data and Information access are key assets for every individual, every company and every state as the digitalization enable efficient work and more efficient business. Thus, Information Technology allows process optimization and industrialization of anything ranging from railway track switching, to air traffic control, from gas and electricity distribution to chlorinating of the water supply. However the current, ever increasing, adoption of digital technology has been accompanied with a lack of understanding of the consequential stakes, especially amongst the young generations. "We don't care how it works, as long as it works." Therefore, there is no awareness that this technology is vulnerable and that without security protection the technology may cause a lot of troubles to the users and economic lost.

Vulnerabilities within the applications on the internet and on the network itself despite the continuous efforts they to be removed will never completely happen, because they're in-built into the internet's very architecture. Criminals use them with developed malware to steal billions of dollars or data and

hacktivists use them to further their political goals. Between 2004 and 2013, over 1 billion records of personal information were stolen or leaked through data breaches of major world organizations.
As a thought experiment, let's imagine what a perfectly secure internet might look like with introduction of severe measure. Users would not be allowed to download or install anything onto their computers. All internet traffic would be monitored and regulated by bots and humans, massively limiting the number of websites individual user could visit. In order to log onto a website the user will need to type in a 100 character password, submit a genetic sample, and whistle a tune for example.
The servers that hold data would be kept in heavily armed fortresses on some isolated places. Even with the presence of all these safeguards in one place, some very clever hacker can overcome the barriers and will find a way to breach through the secure doors.

At first, computer hacking incident was a game, a playful hobby for a few curious, skilled people. As the Internet evolved, these skills became a political or ideological tool in the hands of hacktivist groups who perceived their activity as a legitimate form of social protest (VanOmmeren, Borret and Kuivenhoven, 2014). However, today the most disturbing is the criminal use of networks and technologies, with many organizations seeing loss of billions of USD. According to the UK Cabinet office (UK Cabinet Office »The Cost of Cyber Security Crime«), the cost of cybercrime is about £27 billion per annum to the UK economy. Of this approximately £2.2 billion directly affects the Government, approximately £3 billion directly affects individual citizens, mainly through identity theft and online scams, and UK businesses lose £21 billion per annum. of events every day. These cybercriminal acts include significant security threats targeting customer data, intellectual property and confidential data. Cyber espionage, targeted against both government and industry, has become also a common practice.

To prevent these threats the CyberSecurity Technology in the last 30 years has started to rapidly change the scene of cybercrime. Today cybersecurity technology is shaping the way that technology impacts on business and industry with components that provide more secure processing and work. The term Cyber security is understood as protection of digital systems and assets from crimes. This includes protecting data and preventing undue release and usage for criminal purposes. Protecting data in cyberspace is very challenging. The need to reduce the risk and the cost of cybercrimes is obvious. Security systems and measures provided by the cybersecurity technology have changed the way companies deliver products and services, how people communicate with one another, how organizations make decisions and even the way individuals understand and interact with the digital world around them.

Many of these changes are being driven by the confluence of significant, interrelated trends around cloud, mobile, big data and social networking. While each of these shifts is independently significant, taken in combination, the pace at which is changing is rapid and impactful.

However, just as these shifts had a pervasive organizational impact, the emergence of organized crime, state-sponsored attacks and social activism in the digital world shape the new reality in which security risks are not understood sufficiently as important challenges, although they can often threaten an organization's brand, intellectual property, sensitive business data and financial resources.
The presence of these risks are expected to change the way the organization`s approach for protecting their digital assets. Chief Information Security Officers (CiSos) that care about the organization digital security are now accountable for the organization government and have assumed their role of translator between business leaders and security experts, helping each group to understand the perspective, challenges, requirements and objectives of the other.

2. Building cybersecurity awareness

Network and data protection within an organization enable trust in the technology and in the running processes, but introducing that in the organization is not an easy task. In addition to the technology protection the building a cyber security culture within the company is another important and necessary value for raising trust and competence. As threats become more sophisticated and accurately targeted, their impact on the organization staff is increasingly significant in that context the security measures should evolve from focus directed to the identified fear and the recognized risk as vehicle leading to adoption of mitigation measures (Hendrix, Al-Sherbaz and Bloom, 2016). Establishing and maintaining trust and confidence is a competitive differentiator across industry and government. Security must be managed accordingly to the existing threats and risks. Introduction of practices associated with detection and response to attacks should be an essential, multi-disciplinary part of any organization's security strategy. Important measure in provision of security is building awareness about cybersecurity with education and training. However, provision of cybersecurity education and awareness building is not an easy staff, due to the complexity of the matter and the many different aspect that should be taken in in account, from technology, tools, processes human understating and maintenance.

In that context the education of people and making them to be are aware about the prevention measures like the protection tools from attack, data leakage and any other malware is becoming present in most part of the world. One of the ways how to make this education more efficient and less cumbersome is the use of gaming and serious games in the educational process. Serious Games allow people to practice in a safe and playful way and therefore to develop cyber security skills. According to some authors Serious Games may be a cost-effective solution for educating people and in reducing cybercrimes (Hendrix, Maurice & Al-Sherbaz, Ali & Bloom, Victoria, 2016)

Conducting business and personal duties with ICT tools has become ubiquitous to an interconnected society. Companies usually invest large amounts of budgets for hardware and software controls to determinate and prevent various attacks on company digital assets within. For example firewalls and anti-virus software are updated constantly as the threats and cybercrime attacks evolve with the technology development. In spite of these measures based on the technology, the weakest link in security chain is still the human element whose actions can be considered sometimes as erratic and unpredictable thus posing a threat to the organization they work. Existing security awareness programs aim to equip the users with the necessary knowledge to identify and mitigate threats (www.karspesky.com, 2020). Numerous security awareness frameworks like one suggested by Kapersky prescribes steps to be implemented as efficient and effective security awareness program. These different steps are recommendations are still needed to be further develop and customized in programs for a specific environment and public. It should be noted that currently their different educational methods which include training courses, information passing through newsletters and websites. These contents on the network deliver security knowledge by addressing different users. The nature of these methods sometimes shows that are ineffective as they are considered mundane and strenuous for users who do not have relevant technical background in information technology, which, in turn threaten the success of the offered educational programs. Therefore proficient solution is usually needed for attracting the diverse group of users interested in security awareness training (Labuschagne and Eloff, 2019). Moreover the effectiveness of these programs is usually measured with the application of metrics defined by the security awareness programs.

3. Computer courses and the lack of security topics

In the last decade the security landscape has been fast changing as security research and training is attracting a lot of investment from governments and the private sector. While these efforts are not clearly visible as is the investment in the physical security, but as the computer infrastructure and networks control many vital functions in society, e.g. banking traffic and air traffic efforts in improving the cybersecurity can be found to be remarkable. A number of recent high profile attacks on many organizations have highlighted the importance of the cybersecurity education and it has become clear that training of both the general public as well as the security professionals should become major focus in provision of security and protection of digital assets.

In response, many specialized education programs and funds have been supplied by governments globally, in an attempt to satisfy the immediate demand for cybersecurity skill labour force. Most experts are in an agreement that in order to meet the increased demand for skilled security workers, cybersecurity specific teaching methods need to be prepared and offered. A predominant problem surrounding current teaching practices is the lack of emphasis on more modern Computer Security education in the academic and the business world. It is not surprising the Computer Security topics to not be present in the high school and the higher level educational programs that usually offer just general computer studies (UK Cabinet Office »The Cost of Cyber Security Crime«). In the paper entitled "This is Not a Game" author Mark Gondree and Zachary N. J. Peterson point out that the missing security content within the computer courses, is noting than "the technical complexities and the mundane subtleties of computer security which do not easily lend themselves to a lower-division college curricula".

Computer security is a growing area, and is becoming very important for the safety of any country Currently there are still in the developed countries insufficient students graduating with cyber security experience that are needed to fill the available jobs, while at the same time, the public's interest in security and privacy topics has never been higher. In order to increase the number of people that choose degrees in both Computer Science and Computer Security, it is necessary these topics to be presented to the undergraduates and to the high-school students early in the educational development (Sehl and Vaniea, 2018).

Experiences with the role playing in the training process of cyber security appeared to be a tool that is especially well-suited to training with digital games, especially given the digital nature of cyber security. Games used in the education and training are games with a purpose other than pure entertainment, their purpose is to enhance the learning of the trained subject. As Serious Games have gained increasing interest and augmented use in fields such as project management, healthcare (Arnab, 2013), advertising (Cauberge, 2010), and behavioural change (Dunwell, 2014). Nowadays they are becoming popular tool in the cybersecurity education. Studies have shown that games can not only be effective training tools, but can also be effective in encouraging behavioural change among the iCT users (Hendrix, 2014).

The number of computer games is raising dramatically in line with their increased popularity. Hendrix, Al-Sjerbaz and Bloom (2016) have pointed out with within their survey that the Serious Games are become respected field of application in any level of education. As the field develops rapidly and these developments are taking place both in academic and commercial settings, other scientific studies have been carried out with an aim to classify and assess currently available products dedicated to education on the game market. The empirical studies from Hendrix, Al, Sjerbaz and Bloom (2016) have shown 49 hits of paper dealing with games with topics close to the cybersecurity field. Each of these was inspected by the same authors, for relevance, and they have provided final selection of 28 paper. The findings pointed that the development of cyber security educational games is becoming a new prospective approach in the educational area of serious games. The early stage »cyber security games« were available only in form of a puzzle-based or gameboard form (Android: Netrunner the card game is Available at https://www.fantasyflightgames.com/en/products/android-netrunner-the-card-game/).

The novel cyber security games are today more demanding for the learner and they can be found on variable platforms. Serious games for cyber security education and training can be run as standalone application or on 3D virtual world station or as a simulation tool. Most of them are available on the mobile phones and on personal computers. While the number of studies about the cyber security training games is growing, most of them are still facing efforts to be used for training or raise awareness within the general public.

However, it is important to be noticed that despite the problems in becoming popular Cybersecurity serious games are certainly a part of the new emerging world of education environment that is based on sophisticated technology with elements of entertainment. They have been seen as good supplements for supporting the learning processes due to their capability to increase visualisations and to challenge the student creativity.

However, despite any reservations regarding use of gaming for training, many senior managers at cybersecurity firms or units across the industry find themselves turning to more specific measures to fill their short-term needs and among them is the use of games. The McAfee survey found that 75% of senior managers at cybersecurity firms reported that they would hire a gamer with no experience in the field to train them internally just to meet their projected short-term needs. The talent shortage in cybersecurity poses a large, persistent, and growing problem for both private and public interests, so any efficient method that shorten the education is much welcomed.

4. Cybersecurity Serious Games and the game taxonomy

Nowadays the origin of the term Cyber security is coming from a IT field with multiple and technically complex digital technology and with ever changing aspects due to the changes in the digital world, and as cyber threats can affect individuals as well as large organisations like businesses or governments, it includes aspects of organizational and human behaviour. As a consequence the education of the people for the most basic cyber security principles is a today a must (Le Compte, Eizondo, Watson, 2015). Training new people in cyber security and privacy is a serious problem and as the the global shortage of workers skilled in this area is constantly present. Gamification as one of the most popular approach for training is known as a process of taking a training exercise or other activity and converting it into a game (Le Comptem Eliondo, Watson, 2015). Luckily cyber security is an area that align well with game-type thinking approach used in education. In that context, there is always a digital resource (computer, system, data) which needs to be protected for attack prevention. For protecting the source there are various tools which can be used for a defence from the attacks which in the cybersecurity game the player become familiar with. Serious games have received a fair amount of attention in the field of information security and cyber security, both from academic researchers and in industry as well. One of the most popular examples is the game called "CyberCIEGE" (https://nps.edu/web/c3o/cyberciege), created by the US Naval Postgraduate School (NPS) and sponsored by several US organisations (https://nps.edu/). The game offers a realistic virtual world in which players have to operate and defend a computer network. From a pedagogic point of view, the game encompasses seven fundamental cyber security related topics. The game has also been also the object of many academic publications and has shown good pedagogic benefits. Other examples developed by various US military departments, universities and other organisations, are presented in the study of authors Pastor, Diaz and Castro. (2020). The study is good overview a of the current state of the art of simulation systems for information security education, training and awareness. Although the paper describing the game is focused on simulation systems, the distinction between serious games and pure simulation tools is still quite blurred. This is reflected in the context of the present study that analyse the current state of the art.

Most popular gaming applications are used in the competitions of individuals challenged to solve the security problem and prepare adequate solution. In the 21 siècle the cybersecurity competitions are growing in both popularity and diversity. The Web site CTFtime (https://ctftime.org/) reports that there have been an average of 56 cyber competition events per year since 2013; this is almost one gaming competition every week. The International Capture the Flag (iCTF) game competition reports that the participation steadily increase. In the past five years the participation on averaging doubled compared to prior years. There are three separate US leagues that organize the competition but this regional play culminates in a national competition. DARPA's Cyber Grand Challenge is the latest variation of the cybersecurity game competition organized for training students.." The participants are engaged in a technology demonstration that has a game format. In the midst of this cybersecurity game growing production, it can be noticed that designers, organizers, and researchers are facing some semantic gap when describing and discussing the cyber competitions. Some terms used to describe the cybersecurity games are based on analogy, sometimes stretched to where the relationship becomes weak, like in the capture the flag (CTF), the Jeopardy-style games, quiz bowl games and others. The terminology is still invented but it is still without wide adoption and therefore still evolving in meaning, examples of the terms are : hack-quest, inherit-and-defend, hack-a-thon. The game format is important as well as it is a deciding factor for players, who may be unable to participate in person for non-virtual events (they need to travel), assembling a group for team play can be a problem, or may be the players are unavailable to engage in a full day in a synchronous competition. Thus, at the very least, a common lexicon would help the players and teams to identify competitions aligned with their interests and abilities. Generating such a lexicon is non-trivial, however, as players come to games from different backgrounds, with various motivations and desired outcomes (Dunwell, Petridis, Amab, De Freitas, Lameras, Stewart and Hedrix, 2014). Players may be novice learners seeking to build new skills or practice the learned skills in provision of security.

Framing cybersecurity as an evolving puzzle can change the public perception of the industry, that gamify this complex subject. Meeting that changed perspective with competitive initiatives creates a sort of game-like atmosphere around the industry. The most popular of these competitions are the Capture the Flag (CTF) events. These trials test the ability of participants across a wide range of skills relevant in the security industry. Often these competitions are sponsored by companies like Uber, Walmart, Raytheon, Snapchat, Amazon, or IBM, and are used to recruit promising talent.

It is clear from the known reports that no game on its own can possibly satisfy expectation of every player regarding the upgrading of his/her cybersecurity skills. Imprecision in communicating requirements, outcomes, and mechanics means some players may not be able to identify the games that are appropriate for their goals. To avoid player disappointment, competition on Web sites sometimes try to identify what the players are by clarifying the established language in case is the terminology is confusing or is imprecise .

The most two common factors that are frequently discussed in cybersecurity games are:

- whether the player will be either attacking or defending a network, service, or digital asset,
- whether the player will be attacking other players.

While these factors are more easily characterized at their extremes, they can be imagined as a continuum, encompassing the dimensions of task variety and adversary dynamicity. Task variety refers to the types of knowledge, skills, and abilities players need to demonstrate during the competition. At one end of task variety are games that mix attack/defend mechanics with a variety of domain-specific challenges, typically requiring a team due to complexity and scope; at the other end are games that focus on a narrow variety of skills, like service hardening or reverse-engineering challenges (Gondree, 2016). At one end of adversary dynamicity are games featuring pre-created challenges, where the game adversary's strategy is "baked" into the competition by the designer; at the other end are games where opposing players control the game adversary's strategy, allowing it to be arbitrarily complex and highly dynamic.

Several games have attempted to teach computer-security-terminology and concepts to beginners and experts alike. In this paper we will discuss some of the most popular games, for a more comprehensive review of computer science themed games we refer the reader to a systematic review (Sehl and Vaniea, 2018)

5. Overview of the TULIPS classification of Cybersecurity games

The internet search and the review of various articles done in this study have shown that there is a wide number of video games that teach cybersecurity principles, skills and basic knowledge. For the purpose of this report a CyberSecurity games classification was found at The TULIPS (Technology Usability Lab in Privacy and Security), which has proposed the grouping of the CyberSecurity games into five main groups. They are presented below:

5.1 Capture the Flag Group (CTF)

The CTF stands for the term »Capture the Flag«, which is coming from a traditional outdoor game where two teams each have a flag and the objective is to capture the other team's flag, located at the team's "base," and bring it safely back to their own base. In the cybersecurity play of CTF is a competition between security professionals and/or students that learn about cyber security. The CTF competition is used as a learning tool for everyone interested in cyber security. The game help in sharpening the tools application by the student based on what he/she has learned during their training. It is a competition between security professionals and/or students learning cyber security topics. The attack-defend CTF part of the game is consisted from each team attacking the other team's system, as well as the defend of the team own system.

The two most popular formats of CTF are called jeopardy and attack-defend format. Jeopardy presents teams with several categories of challenges that require technical answers to problems facing areas such as cryptography, hacking, forensics, networking, and programming. Attack-defend challenges put two or more teams against each other enabling them to use any means necessary to take over and maintain control of an isolated network of computers. Competitive CTF events can be found throughout the industry, with no-table examples like the US Cyber Challenge, the National Collegiate

Cyber Defence Competition, or at larger tech meetings like Google's Chromium Conference. Those players who rise to the top of these competitions become highly thought experts by the companies who watch them intently. Rather than a job interview, excelling at a major competition can prove to be a method of entering the industry and getting good job position.

One of the example from this group is the free on-line available game known as picoCTF, created by security experts at Carnegie Mellon University. The game consists of a series of challenges centred around a unique storyline where participants must by reverse engineering to break, hack, decrypt, or do whatever it takes to solve the security challenge.

5.2 Firewall Group

Certain topics in Computer Security, for example firewalls, seem to be very difficult to be understood by beginners. Firewall is a piece of software (or hardware) that, if correctly setup, can protect the network from being successfully attacked over the internet (or from within the other parts of the network).

It is an important system designed to prevent unauthorized access to or from a private network. It is essential a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network. Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks and run on the network hardware supported by specific software. Host-based firewalls run on host computers and control network traffic in and out of those machines . (Cheswick, Bellovin, and Rubin, 2003)

Managing the Firewall policy rules for a large network is a very challenging task, even for a skilled system administrators. Learning these skills requires to learning the IP table rules[1] through a mission-based game. The literature review has shown that several cybersecurity games have as a focus on the technical firewall topics such as chains, packets, and ports. The understanding of the firewall requires the students or the learners to have a fundamental knowledge about the firewall terminology and to be capable to build a strong mental model of how the firewall works internally. (Sehk and Vaniea, 2018)

One of the games from this group is the »Permission Impossible« game , build with Unity 3D software game engine, it is free to for playing. The game was designed to be highly accessible to a general public audience

[1] IP Tables is a user-space utility program that allows a system administrator to configure the IP packet filter rules of the Linux kernel firewall, implemented as different Netfilter modules.

5.3 The General Group

The general group games have focus on the general knowledge about cybersecurity and are intended to be applied for learning by non-technical, average-security-knowledge audience (users). These games do not address so-called typical technical computer skills and cybersecurity knowledge background. To be more specific, the knowledge that particularly involves coding, hacking, writing program scripts and building a firewall, are not part of their educational topics. The games are presented mostly as an adventure game with story-telling scenario with an intention to facilitate the understanding of cybersecurity way of incidents prevention. Usually, during the game, there is in the background a fictional story about the high-risk security in the digital interconnected world. Players usually, based on the game content, need to make the right and crucial decisions in order to bring the game to the end. The game flow within this group of games is usually in a form as pre-played scenario, or mind-puzzle game, where, the user success depends on the deciding/selecting the right decisions. In particular, the General group of CyberSecurity games is dedicated to the audience with no specific IT background or people who are average-based IT user, such as internet users, kids, high school students and people whit soft skills of IT knowledge, such as entrepreneurs, project managers, CEOs etc. The General CyberSecurity games are usually free to be used and web-based applications in order to be available to the widest public audience.

5.4 The Networking group

In this group, the games are based on the simulation approach with an aim to teach the basics skills and knowledge about how computer networks function, with emphasis on the security issues. A computer network is a digital telecommunications network for sharing resources between nodes, which is in form of computing devices that use a common telecommunications technology and protocols. It is a set of computers connected together for the purpose of sharing resources. The most common resource shared today are the devices connected to the Internet, which are estimated to be more than five billion. Shared resources are also a printer or a file server or an IoT (internet of things) device. Connected computers can share resources, like access to the Internet, printers, file servers, cameras, sensors and other devices. The sharing data and storage of data on servers or personal computers connected to the internet is explicitly vulnerable to cyber-attacks. There are several video games suitable for teaching Network Security competences, such is the game CS4G Netism. The game is a sort of simulator, intended to be used by players that learn how to perform attacks in the same manner as the real hijackers do and see how the attack process works in the Netism simulator. This approach enable the learners to understand more easily how to prevent or fight again attacks. CS4G Netism is a free to play application, it can be visited at https://netsim.erinn.io/

5.5 The Table Top group

The final group from the list of five is the table top group. The table top group consist of the games that can be played in a real physical form (meaning not digital and installed on computer or mobile devices). The table top games are mostly similar to monopoly, dunges and dragons games, by using set of cards. These games use »dealing-card« principles like playing puzzle or exchanging cards. Each game consists of the dealing-card pack, where, depending on a subject of the game, players can use them in order to hack or defend the network services or information systems. Each card has a particular point in a form of a distinguished skills and abilities. Table Top CyberSecurity games can be played by the non-experts of cybersecurity or the novice experts and beginners. The game master (the person who designs a game, designing the game-scenario) is responsible for preparing the strategic situation of the game-play and also the one who is dealing with the deck. For the master is required to have some cybersecurity knowledge, in code-base background or hacking system.

rt

CONTROL-ALT HACK
WHITE HAT HACKING FOR FUN AND PROFIT
FRANZI
ROXANA
KARL
1 HACKER CRED
5 HACKER CRED
$2K
ATTENDANCE
ENTROPY
MISSION

6. Presentation of the selected Cybersecurity games

The literature that has been found by browsing the world wide web is presenting the games that have been developed or been used in an academic environments. These games are:

TiER1, Anti Phishing Phil Security games by Next Generation Security (NGSEC), CyberCIEGE, PicoCTF, Control-Alt-Hack, (d0x3d!), Baltic Cyber Shield (BCS) international cyber defence exercise, Internet Hero, Security awareness program, CyberNEXS, OnGuard, Budd:e, Nsteens, Carnegie Cadets, McGruff, FBI Cyber Game, CyberSecure Your Health Practice, PBS Cybersecurity Lab, The Cyber Security Challenge UK, Game of Threats, High School Cyber Security Game – global cyberlympics, CyberProtect, Cyphinx, Project Ares and many more.

The level of complexity of these games differ very much, as some of them are suitable just for children audience, with intent to teach young children how to stay safe on internet. The other games are more demanding as they are focused on obtaining the fundamental cybersecurity skills and knowledge. For the purpose of this study we have selected several games from each group and for each level of required knowledge. The selection of the games was led by intention they to be effective, and enjoyable to a variety of audiences.

The following selection of the CyberSecurity games presented below are:

- Targeted Attack: The Game
- Cybersecurity Lab
- ThreatGen: Red Vs. Blue
- CyberSIEGE
- Permission Impossible
- Data Center Attack
- CS4G Netism
- Firewall administration: The Game
- Cyber Awareness Challenge
- Keep Tradition Secure
- Zero Threat
- Cyber Threat Game

6.1 Targeted Attack: The Game

Targeted Attack: The Game is an immersive simulation game created by Trend Micro ltd (www.trendmicro.com) for student training to test system cybersecurity abilities and to make the right decisions for avoiding the devastating consequences of a major data breach.

Targeted attack in the game is built on the principles of adventure game, which means, it is a type of video game in which the participant plays a fantasy role in an episodic adventure story. More than any other genre, the adventure games depend heavily upon their story and the setting of a compelling single-player experience. This game offers to the player the unique chance to step into someone else's shoes and to find out if the player is good enough to come and face with critical challenges of data breach.

The game transfers the player into the role of the CIO person who works for in a global organization called The Fugle, responsible for making the first release of a biometrically authenticated mobile payment application. The player in his/her role of CIO has to steer the project through its final stages, dealing with the internal security team, such as are the player's colleagues.

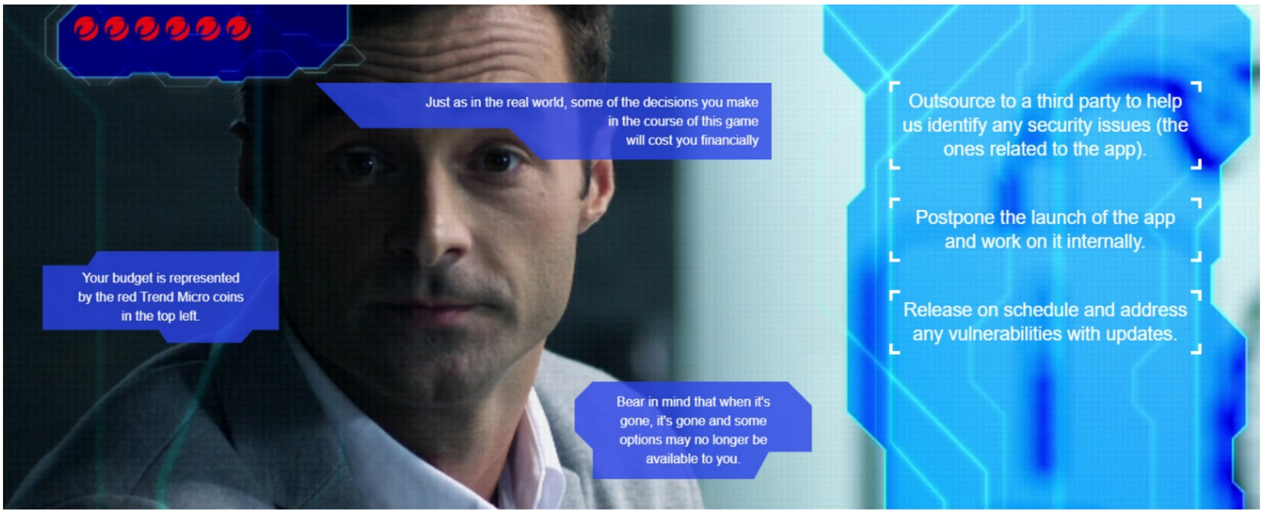
The main task for the player can be formulated as »There are many competitors and individuals out there who would love to get their hands on the data held by your organization at such a critical time. Can you make the right choices to prevent this? Can you keep the project on time and on budget? Can you protect your company from attack?«

When the game begins the player has to steer his/her organisation through the final days of the application launch process, safeguarding intellectual property, and financial data and securing the corporate network against day-to-day threats.

His/her decisions are cruicial and the security of the company and success of its ground-breaking technology is onplayer's shoulders, and relies on the best efforts of player's virtual team. Constrained by budgets the player will have to spend wisely, planning for the unexpected, yet meeting the demands of the executive team. In making his/her own decisions, the player has the support the virtual characters team that introduce the player to the security measures in the process of making decisions. He The player must take care of the corporate security and the customers' privacy, he/she is helped by Randall his "right hand man". The team helping the player has few members. Mellinda is – the Fugle CEO. She develops and drives the entire corporate strategy. One of the most visionary CEOs in the industry are those that are turning ideas successfully into reality. Vanessa is a marketing director. She has an MBA in Marketing and Communications from Harvard University and owns professionalism personified. Vanessa knows all about marketing in the InfoSec sector and beyond. She is the inspiration and leader behind every Fugle marketing campaign. Julian is an PR Manager. The one and only, Julian has been in the industry for more than a decade and was last year awarded "Best PR Manager" by the Journalists' Review. Reporting to Vanessa. Julian is always friendly, always professional, always ready to help the media do their job. And last but not least team member is sergeant Harrison. He does not trust new technologies, still believing in traditional investigation methods; a very thorough detective who will go on make a great career in the Police Department.

The game is shown as a story telling interface, which means the dialogue's among the team members are pre-recorded, and the answers to the questions are available in the quiz-a-like form. When the dialogue is finished with player's virtual team personnel, the player is set to choose one of the 3 or 4 available answers.

The game itself does not support the technical cybersecurity skills (such is teaching the programming and inspecting the code the code) that the player should develop during the cybersecurity training, yet with the storytelling and narrator components, the game teach the future managers, entrepreneurs or new-to-come CIO's, enable developing the necessary knowledge and answer to the question what-is-to-take and enable the learner to get the better and sufficient insight of the cybersecurity nature in the company organization.


Just as in the real world, some of the decisions you make in the course of this game will cost you financially

Your budget is represented by the red Trend Micro coins in the top left.

Bear in mind that when it's gone, it's gone and some options may no longer be available to you.

Outsource to a third party to help us identify any security issues (the ones related to the app).
Postpone the launch of the app and work on it internally.
Release on schedule and address any vulnerabilities with updates.

Fig. 3.: The Screenshot of the GAME's GUI (Game User Interface)

6.2 Cybersecurity Lab

NOVA Labs is a free digital platform that engages teens and lifelong learners in games and interactive settings that foster authentic scientific exploration. The platform predicts solar storms and constructing of renewable energy systems for tracking cloud movement and designing RNA molecules. NOVA Labs participants can conduct investigations by visualizing, analysing, and sharing the same data that scientists use.

The Cybersecurity Lab is a game designed by NOVA Labs intended to teach people how to keep their digital lives safe, spot cyber scams, learn the basics of coding, and defend against cyber-attacks. Players assume the role of the chief technology officer who is starting-up social network company that is the target of increasingly sophisticated cyber-attacks. In the game, players must answer to challenges that strengthen their cyber defences and thwart their attackers. The Lab also features stories of real-world cyber-attacks, a glossary of cyber terms, and short animated videos that explain the need for cybersecurity, privacy versus security, cryptography (cyber codes), and what exactly hackers are and what are they doing.

Alongside with the players is their virtual friend and colleague—a brilliant, business-savvy entrepreneur helping them it to grow their tiny company into a global empire. To do this, players must complete challenges to strengthen their cyber defences and thwart their attackers. There are four major gameplay components: a coding challenge, a password challenge, a social engineering challenge, and a series of cyber battles.

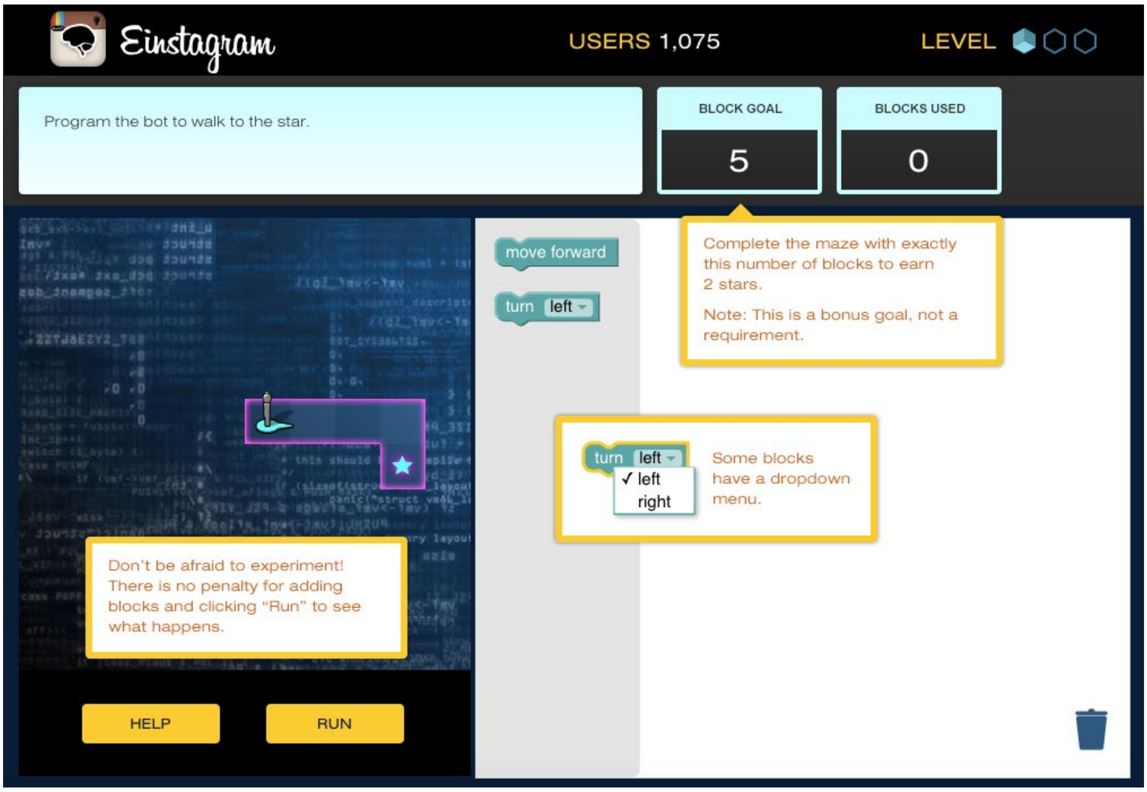
Coding Challenge: This part is introduction to very basic coding skills. The players are asked to program a robot to navigate in a maze, using drag-and-drop commands. This challenge is an introduction to a basic computer programming. Computer code is usually written in text, but in this challenge the players are using Blockly, a visual computer programming editor created by Google that uses drag-and-drop blocks that can be stacked together to create a computer program.

Password-Cracking Challenge: A series of "password duels" teach players the basics of how attackers try to crack their passwords and how the players can make better, more secure passwords. A Password is the most common way people prove their identities online, so using a strong password is essential for keeping digital information safe. In this challenge, players face a series of "password duels" that teach the basics of how attackers might try to crack their passwords and how they can create passwords that are more resilient to be cracked and secure.

Social Engineering Challenge: Players are presented with two apparently similar emails or websites. They must first identify the differences between them and then decide which one is a scam attempting to steal some information or money. This challenge also includes a number of audio recordings and transcripts of phone calls, and players have to decide if they should trust the caller or not. Scammers try to trick people into handing over sensitive information and downloading computer viruses from emails. In this challenge, players will learn to spot scam emails, websites and phone calls. They will complete the challenge armed with practical tips that will help them avoid becoming victims of social engineering scams.

Network Attacks: As their companies grow, the players are pushed to buy defence tool to defend themselves against a series of cyber-attacks. The better that players answer to the three challenges, the more resources they'll get to buy defences. By completing the challenges, players are enabled to buy tools against a series of cyber-attacks that reflect the types of attacks that real companies and institutions often are victim. Players learn about a range of cyber-attacks and how to effectively defend institutions from them.

Each Lab run is unique, and focuses on a different area of active research. But all of them illustrate the key cybersecurity concepts with engaging and informative videos and guide the participants to answer correctly to scientific questions or design solutions to current problems.



Program the bot to walk to the star.

Complete the maze with exactly this number of blocks to earn 2 stars.

Note: This is a bonus goal, not a requirement.

Some blocks have a dropdown menu.

Don't be afraid to experiment! There is no penalty for adding blocks and clicking "Run" to see what happens.

Fig. 4.: A screenshot of the Cybersecurity Lab: programming the robot

6.3 ThreatGEN: Red vs. Blue

ThreatGEN: Red vs. Blue is the industry's first multi-player strategy computer game where players compete against each other, head-to-head, to take control/maintain control of a computer network. In addition to other games, it is worth mentioning that this is not a fiction-based game like those found on the consumer gaming market. The game is based in real-time environment, which means is running in live technology, player vs. player in "gamified" training simulator, designed to teach cyber security skills in an immersive and interactive applied learning environment. The game provides to the students a real-world cybersecurity concepts, methods, strategies, and skills.

ThreatGEN: Red vs. Blue game is played much like popular global domination board games. Rather than a world map, the "game board" consists of a computer network, which players compete for taking control over it. Instead of simulated computer terminals, players choose and commit actions using "action cards" similar to a trading card game.

Every single member of the development team for this game actually comes from the cybersecurity (or INFOSEC) community. Most of them work, or have worked, for years as cybersecurity professionals, and will usually remain active members of the community. The developers of this game are Clint Bodungen and Aaron Shbeeb and they are authors of the book entitled, “Hacking Exposed: Industrial Control Systems”. ThreatGEN: Red vs. Blue was developed and tested based on their experience that includes the results of the feedback from more than 300 beta testers in the cybersecurity community. The authors plan to continue to make regular updates based on continued feedback, making this truly a game by the community, for the community.

ThreatGEN Red vs. Blue is also the only training tool in the world that exercises practical application of “higher-level” and more strategic concepts such as building cybersecurity programs, risk mitigation strategy, and much more.

The end game objectives can vary depending on how the user has configured the current game session. Blue Teamers (Defenders) are required to hastily build up the organizations layers of defines while facing real world budgetary and resource constrains. Red Teamers in the game (Attackers), much like in the real world are constantly gathering intelligence about their target, and are prodding and probing the network to find just one (or many) vulnerabilities so that they could further gain a foothold on the Blue Teamer's network. Once the player has selected the chosen action, depending on its complexity the action will require resources (and money from the Blue Teamers), along with waiting an X number of turns before the action has been successfully performed.

The game is extremely affordable as it allows ThreatGEN to reach out to all Information Security professionals from around the world.

ThreatGEN: Red vs. Blue has the possibility to build a whole Cybersecurity Gaming Communities as the game is available in Multiplayer Mode, so the player plays with the other gamers waiting in the game

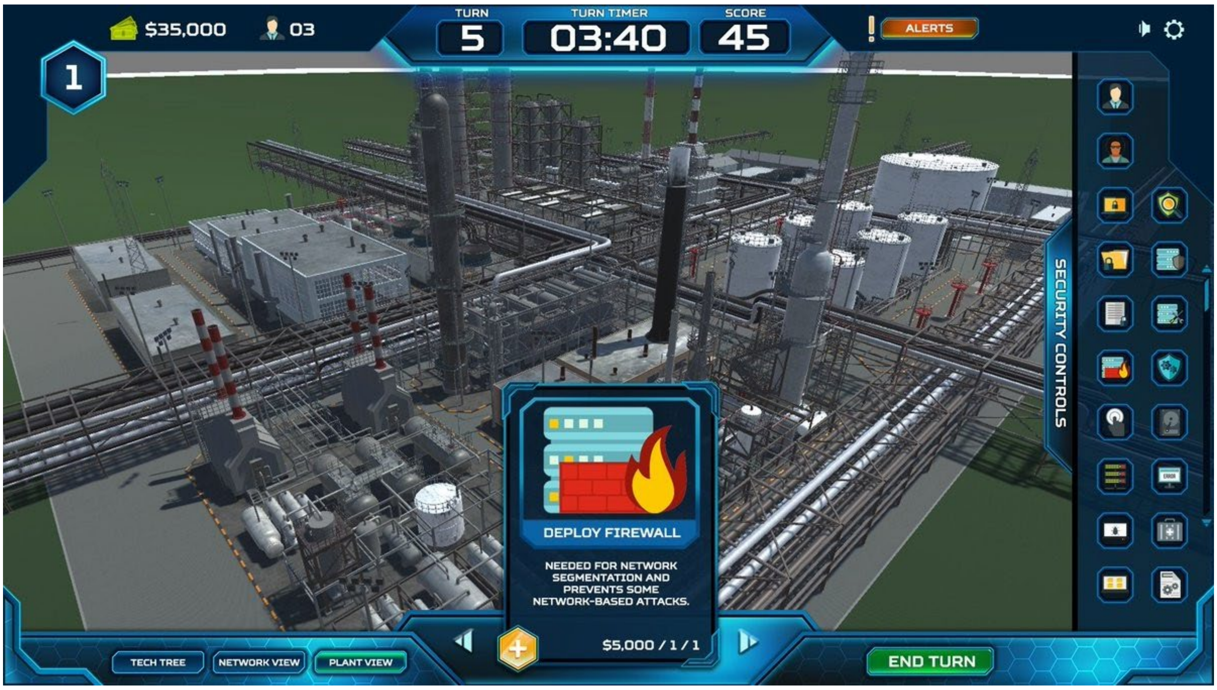


Fig. 5.: A screenshot of Blue Vs. Red Game

6.4 CYBER Siege https://nps.edu/web/c3o/cyberciege

CyberCIEGE is an innovative video game and tool to teach computer and network security concepts. In 2005, the Naval Postgraduate School released an U.S. Government version of CyberCIEGE, a video game intended to support education and training in computer and network security. Simultaneously, the collaborators of the school at Rivermind, Inc. made a version available to non-government organizations.

The aim of the game is to enhances information assurance and cyber security education and training through the use of computer gaming techniques such as those employed in SimCity™. In the CyberCIEGE virtual world, players spend virtual money to operate and defend their networks, and can watch the consequences of their choices, while under attack (Wikipedia, 2020).

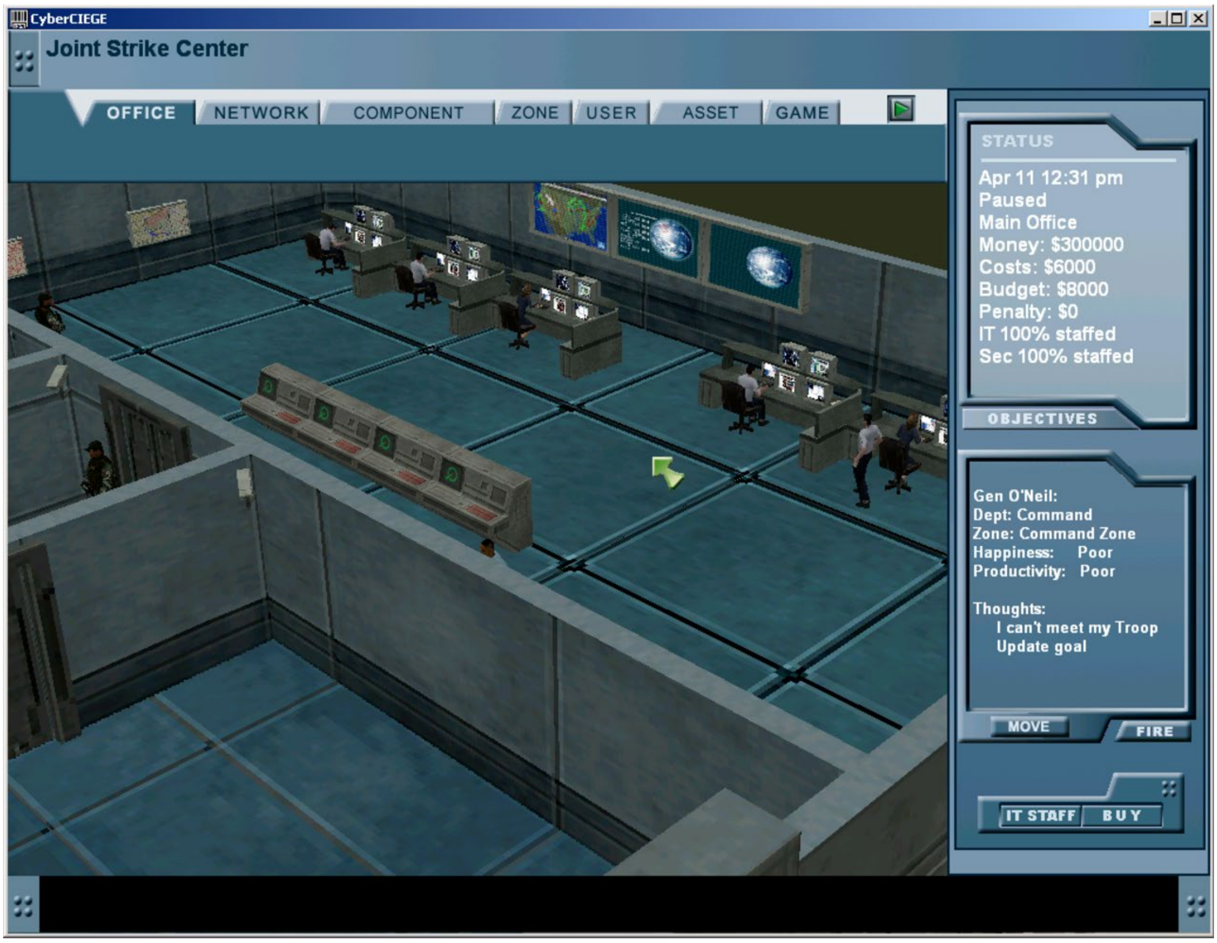
In its interactive environment, the CyberCIEGE covers significant aspects of computer and network security and defence. Players of this video game purchase and configure workstations, servers, operating systems, applications, and network devices. They make trade-offs as they struggle to maintain a balance between budget, productivity, and security. In its longer scenarios, users advance through a series of stages and must protect increasingly valuable corporate assets against escalating attacks.

The CyberCIEGE game engine consumes a “scenario development language” that describes each available scenario in terms of the user’s needs (and their goals), assets (and their values). The initial state of the scenario is described in terms of pre-existing components, and the conditions and triggers that provide the flow to the scenario. The game engine is defined with enough fidelity to host scenarios ranging from e-mail attachment awareness to cyber warfare.

The game is designed as a "construction and management simulation" set in a three-dimensional virtual world. Players build networks and observe virtual users and their thoughts. Each scenario is divided into multiple phases and each phase includes one or more objectives the player must achieve prior to mov to the next phase. Players view the status of the virtual user’s success in achieving goals (i.e., accessing enterprise assets via computers and networks). Unproductive users express unhappy thoughts, utter comic book style speech bubbles and bang on their keyboards. Players see the consequences of attacks as lost money, pop-up messages, video clips and burning computers.

Students play the role of a decision maker for some enterprise such as a small business or military command. The game includes over twenty scenarios that confront students with a series of choices that potentially affect the security of enterprise assets. The figure No. 6 is a screen shot from one scenario. Students make decisions within a three-dimensional office environment populated by game characters who need to access enterprise assets to achieve goals and thus advance the student through the scenario. Sometimes these goals require the purchase of servers or workstations, other situations require network interconnections to permit sharing of assets between virtual users. An in-game economy rewards the student when users achieve goals and the economy suffers when users fail their goals. The virtual assets have associated motives whose values drive the game's attacks which may include Trojan horses, trap doors, insiders, configuration errors, un-patched software flaws, weak procedural policies and poorly trained users. Students identify vulnerabilities and mitigate them via deployment and configuration of simulated protection mechanisms including firewalls, user authentication mechanisms, operating system access controls, biometric devices, VPNs and PKI based application security such as email encryption. Some scenarios also require choices related to physical security (e.g., hiring guards), procedural policies and user training. CyberCIEGE has been in use for six years and has been requested by over four hundred educational institutions worldwide (Thompson, 2011).

CyberCIEGE includes configurable firewalls, VPNs, encryption tools and access control mechanisms. It includes identity management components such as biometric scanners and authentication servers. Attack types include corrupt insiders, trap doors, Trojan horses, viruses, denial of service, and exploitation of weakly configured systems. Attacker motives to compromise assets differ by asset and scenario, thereby supporting scenarios ranging from e-mail attachment awareness to cyber warfare.
Development of CyberCIEGE was 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 Defence, and the National Science Foundation. Numerous NPS students have participated in tool and scenario development. CyberCIEGE is available at no cost to agencies of the US Government by contacting cyberciege@nps.edu. Educational licenses are available at no cost to educational institutions. Contact cyberciege@nps.edu. If you are a student, you can ask your teacher to request the game.



Apr 11 12:31 pm
Paused
Main Office
Money: $300000
Costs: $6000
Budget: $8000
Penalty: $0
IT 100% staffed
Sec 100% staffed

Gen O'Neil:
Dept: Command
Zone: Command Zone
Happiness: Poor
Productivity: Poor

Thoughts:
I can't meet my Troop
Update goal

Fig. 6.: A Screenshot of the game: CyberSIEGE

6.5 Permission Impossible

Permission Impossible, an online game designed to teach people both with and without a computer science background about firewalls. The aim of the game is to introduce the novices about basic firewall terminology and concepts as well as how to build a firewall rule set to enable incoming and outgoing packet traffic.

Permission Impossible provides scaffolded learning through increasingly complex levels. Initial levels provide detailed instruction, with later levels progressively providing less details, less intuitive missions, and finally removing the colour hints from the interface completely. Once The user start to play a game, there is the avatar called Roboto, who is guiding the user through the game. The Roboto provide the user different tasks and hints how to complete the different tasks in order to complete the current level.

Instruction screens provide the story line of the game as well as context, explanation of the terms, and the details of missions. The user is initially greeted by “Roboto” who wants help ensuring “that all the valuable data exchanged between different computers is delivered in the correct fashion.” Roboto then proceeds to explain how data is transferred using “packets” and how the flow is managed by a firewall. He would like the user’s help in setting up the firewall. All instructions and all missions are given by Roboto on instructional screens. The Player must complete the next 10 Levels of knowledge:
Level 1: introduces the policy building interface as well as the basic concepts of having different rules for the packets coming in and going out. The initial mission is designed to be easy to accomplish. The

user is asked to drop all incoming packets and allow all outgoing ones. The building interface presents them with only two blocks: ACCEPT and DROP.

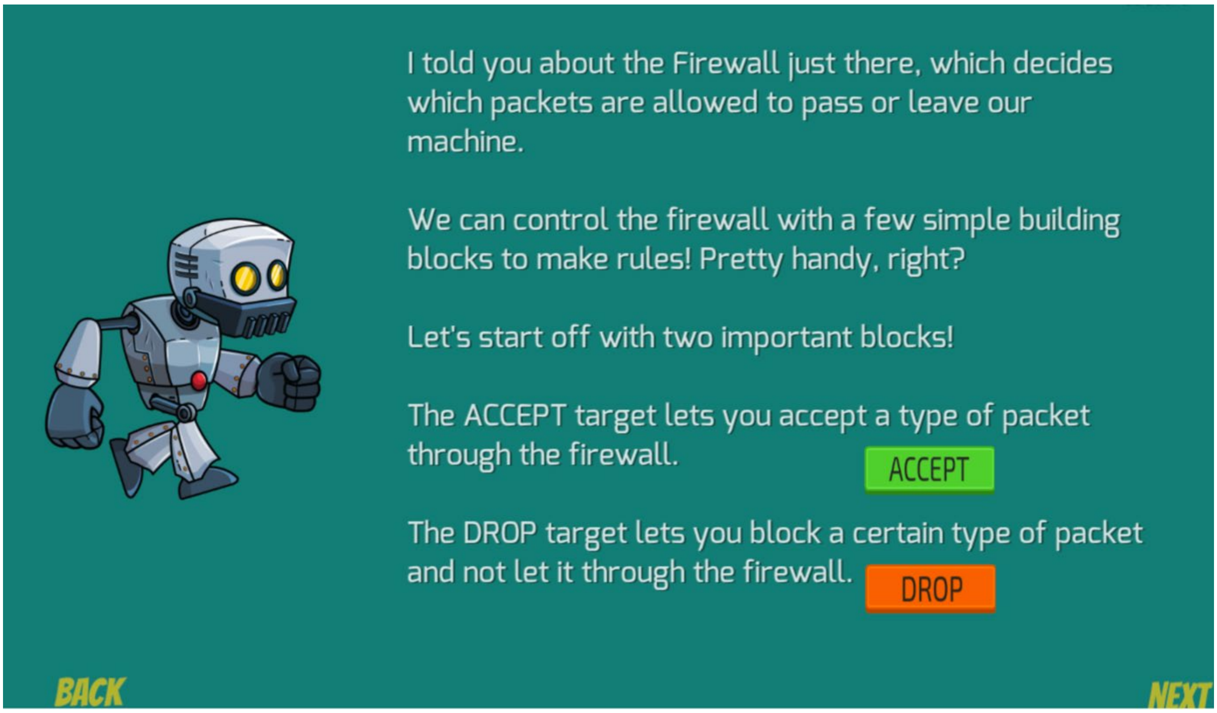
Level 2: introduces the idea of having more than one rule in a chain and that rules are executed in defined order. The user is asked to setup the input chain to allow new and established connections with a destination of port 80, and the output chain to allow established connections with a source of port 80. Both chains should have a default drop rule. Roboto clearly describes the exact rules he would like enacted, including images of the blocks to be used. Roboto explains that these rules will allow the use of the “web” but does not elaborate about services.

Levels 3-7: each of these levels introduces a new protocol with Roboto explaining what the protocol is and how it is used in networks. Introduced protocols are: SSH, FTP, Domain Name System (DNS), SMPT, and SIP. In these levels Roboto uses words to explain what he wants the user to do.

Level 8: combines the knowledge about the services and the ports learned so far and introduces the concept of multiple complex rules.   user is asked to set rules for both web (80) and SSH (22) traffic as well as setting a default policy.

Level 9: takes a different approach from the previous levels and asks the user to implement a default policy of ACCEPT. The user is also instructed to block a specific IP address that Roboto describes as being malicious in the instructional screens.

Level 10: uses all the knowledge the player has gained. Roboto has an emergency and asks the player to “construct sensible rule set” without any detailed instruction. It also removes the colour hints and includes a IP address to assess whether the player understands the concept of a default.



I told you about the Firewall just there, which decides which packets are allowed to pass or leave our machine.

We can control the firewall with a few simple building blocks to make rules! Pretty handy, right?

Let's start off with two important blocks!

The ACCEPT target lets you accept a type of packet through the firewall.

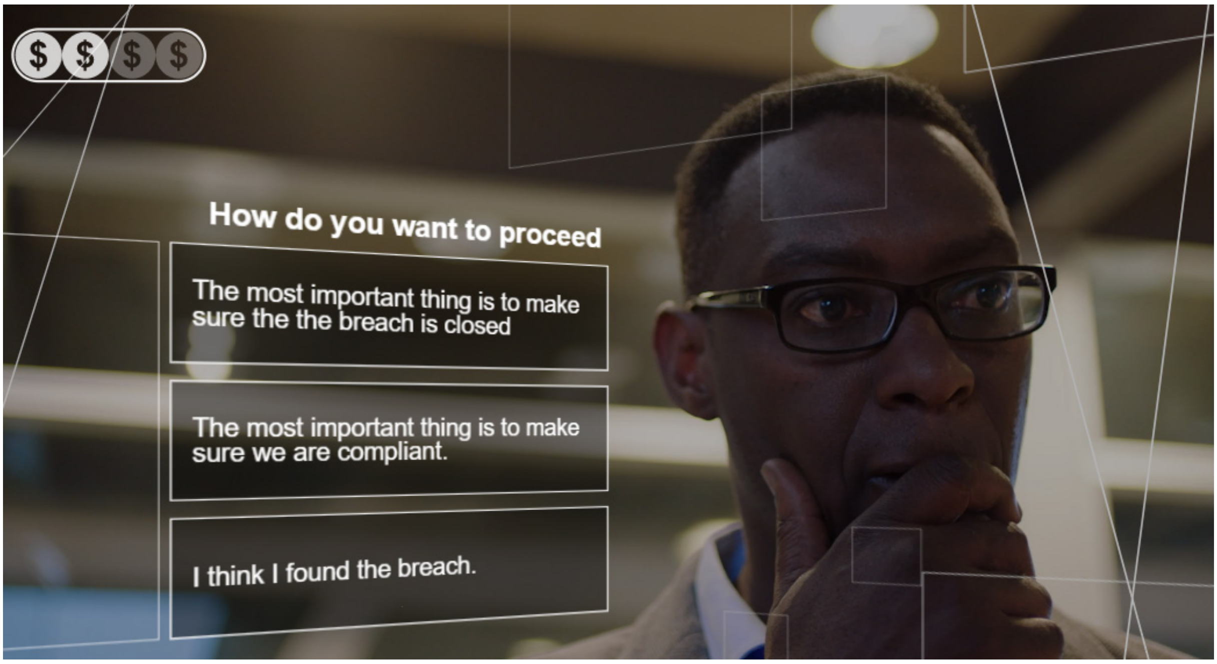
The DROP target lets you block a certain type of packet and not let it through the firewall.

Fig. 7: The player's guide and assistant through the game: Roboto.

6.6 Data Center Attack: The Game

Data Center Attack is the game for learning the cyber threats and cyber-attack situation in the real world scenario. A cyber-attack is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset. A cyberattack is also understood any type of offensive manoeuvre that targets computer information systems, infrastructures, computer networks, or personal computer devices.

The Data Center Attack game is a choose-your-own adventure style game where players play the role of a CISO (Chief information security officer) making decisions for a hospital to prevent hospital computer system to be cyber attacked. The story takes place in the hospital where the player is giving the chance to prevent a data center attack from becoming the stored critical patient data a hostage. Game starts out with a worst-case scenario but then moves onto very realistic situations where the main character- the player is asked to make a sequence of decisions in realistic situations. Wrong choices of the player could result in ransomware hijacking player's patient data and putting lives at risk. Right choices will show what happens with DevOps and IT (hospital departments in the game) work together to enable further allow the doctors to see the patient data, and the hospital to run as expected. The game is based on numbers of video, that are explaining what the story is about. In the introduction video, player finds himself/herself in the emergency hospital. The patient who was the victim of a multi-vehicle accident is being transported into the emergency room, where time is crucial for patient to be rescued. The doctors and nurses have all the patient data available on computer, but when they run the computers, the system frozen up because it is corrupted. The all staff get the message that the computer system has been encrypted by secret hacker. The CISO called the outside security servicer and announce that the system has failed due to wrong decisions. Then game puts the player back in time in order to fix the system security and this time allow the CISO to make the right decisions. The game was developed by Trend Micro corporation. The game flow is based on pre-recorded video scenarios where ideologues are shown between hospital workers, the director, doctors and the security team. Based on the dialogue's, the player retrieves the useful information about the hospital cyber security situation, in order to make the right decisions, in the form of the »quiz« questions. The better decisions a player makes, the more bonus money he/she raises.



How do you want to proceed

The most important thing is to make sure the the breach is closed

The most important thing is to make sure we are compliant.

I think I found the breach.

Fig. 8.: A Screenshot of Data Attack the Game

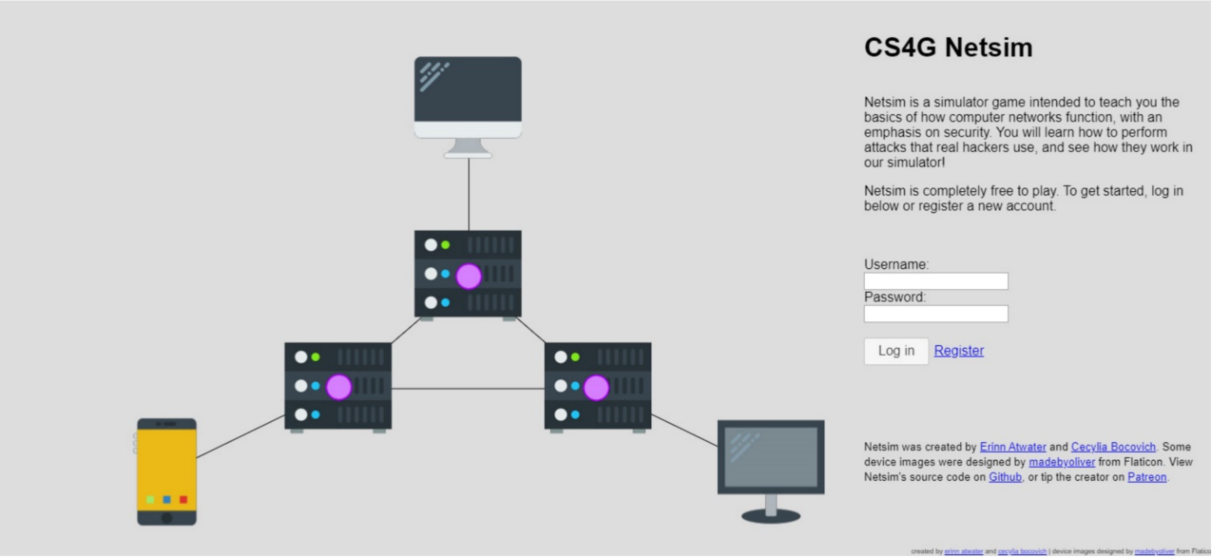
6.7 CS4G Netism

Netsim is a web application implementing a real network simulator, with gamification achieved by offering to the players the ability to craft arbitrary packets and inject them into the network, with the goal of achieving various network reconnaissance/hacking objectives. Players work through a series of levels, slowly introduced by the simulator to network basics, and building up attacks inspired by real network vulnerabilities use, such as address spoofing, denial of service, and surfs attacks. By playing the game, the player can learn how to perform attacks that real hackers use and see how the attacks works in a simulator. Each advancing level of the game is accompanied by a tutorial that describes how the concepts work in real life, explaining the objectives of the level, and giving hints about how to achieve these objectives. The intention of the game itself is to drive interest in computer science, and particularly computer networks and security, by encouraging students to become "hackers" in a realistic game.

The game can be played with a single player. It is targeted at high school students. Netsim levels are composed with three computer objects: Devices, Links, and Packets. Each level has a pre-specified layout of Devices and Links that connect them, representing a network topology. Devices include both computers and networking equipment such as modems, switches and routers. These Devices can only send Packets to each other if they are connected by Links. Some Devices are specified by the level definition as player-controlled, which means the player "owns" that device and can send Packets from it. These player-initiated Packets are created by the player specifying packet header fields in a Graphic User Interface (GUI), and then launching them at any point during the simulation. Other Packets can be pre-specified by the level definition itself and launched at specific simulation times, or can be sent by Devices according to their device script. For example, most devices respond to all ping packets; when received, their script will send a response Packet to the device that sent the ping. To play the game, players must specify headers that manipulate the Devices into sending/receiving Packets (Atwater, Bocovich, Hanartner and Goldberg, 2017).

To play the game, players must specify headers that manipulate the Devices into sending/receiving Packets configured in a certain way (as specified in the level definition). For example, players learn in an early level that the "source IP address" need not be written honestly; they are free to send Packets with spoofed source ad-dresses to impersonate other Devices on the network. Towing this level, they must send a spoofed packet to the intended target, which triggers the win-condition and al-lows them to progress to the next level. The interface for the game (shown in Figure) is that of a typical simulator game: it can be paused, slowed down, and restarted. Pausing is a key element for playing the game, as it allows players to take their time and in- Devices and Packets by clicking on them. This allows them to view the attributes of any Device (by inspecting merely its IP address) or Packet (with all of its packet headers, which they may need to copy.

Netsim was created by Erinn Atwater and Cecylia Bocovich.



CS4G Netsim

Netsim is a simulator game intended to teach you the basics of how computer networks function, with an emphasis on security. You will learn how to perform attacks that real hackers use, and see how they work in our simulator!

Netsim is completely free to play. To get started, log in below or register a new account.

Username:

Password:

Netsim was created by Erinn Atwater and Cecylia Bocovich. Some device images were designed by madebyoliver from Flaticon. View Netsim's source code on Github, or tip the creator on Patreon.

created by erinn atwater and cecylia bocovich | device images designed by madebyoliver from Flatico

Fig. 9.:The screenshot of free web-based game CS4G Netism

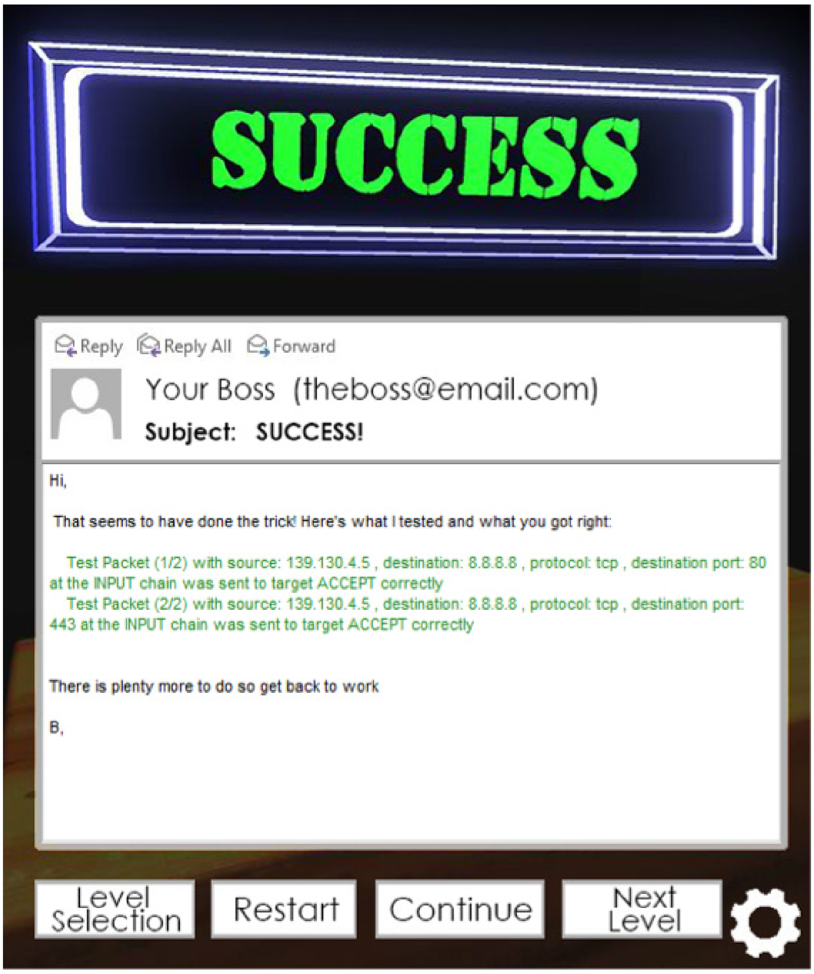
6.8 Firewall administration: The Game

A Firewall administration (available at https://sites.google.com/site/firewallgameinf/) is a flash game designed for firewall administration, specifically learning about IP tables commands. In the beginning the game sets in the beginning the difficulty level of instruction that the player will receive when given an in-game task. There are three difficulty settings: Hard, Medium, and Easy. The player can choose one of the setting based on his/her confidence in their current skill set and background knowledge. Then the player takes the role of the administrator in the company, where he/she receives an email from the Player's boss, explaining the situation as an urgent issue with the firm firewall, as nobody of the employees can access the internet and the firm network. Instruction screens provide the story line of the game as well as the context, explanation of the terms, and the details of missions.

Once a level is selected, the player receives an instructional briefing, as shown in Figure No. 10. The briefing describes the task that must be completed for the player to successfully complete the level. At this screen, there are three actions the player can take. After reading the description, the player may decide to not take the offered level due to many reasons. Reasons may include, but are not limited to: previously completing this level, already possessing the knowledge being taught in this level, or not having the required knowledge to proceed. As such, the option is to return to level selection is given gain for changing the difficulty setting. A player may decide to return to difficulty selection if he/she does not fully understand the instructions given, and would like an easier guidance description. Lastly, the continue button takes the player to the command line screen to complete the given task. The instructions are posed as an email from the players boss. This type is a sort of playing situation, in which the player assumes the role as an employee being assigned tasks from his/her employer and the task required needs to be implemented for several reasons. Primarily, one of the game goals is to emulate the experience of being a security system administrator.

The player’s task is to set up the default policy for incoming and outgoing packets that should be dropped. After reviewing the e-mail letter with requests from his/her boos, the player goes to the next command line screen, where the player get the task to edit the firewall settings using the command line and to submit the directed rule set for evaluation. The lower portion of the screen contains an in-game command line. A command line is a mean for interacting with a computer program where the user issues commands to the program in the form of successive lines of text. The in-game command line behaves similarly to a real command line, with the exception that only the IP Tables (a user-space utility program that allows a system administrator to configure the IP packet filter rules of the Linux kernel firewall) are supported. The input is then passed to the control logic system, which was built to mimic the IP Tables application. The input is then analysed, a response is generated, and if the command input is valid, the appropriate action is taken on the firewall.

The start screen of the game is a user's first impression, and should be visually appealing.



Your Boss (theboss@email.com)

Subject: SUCCESS!

Hi,

That seems to have done the trick! Here's what I tested and what you got right:

Test Packet (1/2) with source: 139.130.4.5 , destination: 8.8.8.8 , protocol: tcp , destination port: 80 at the INPUT chain was sent to target ACCEPT correctly

Test Packet (2/2) with source: 139.130.4.5 , destination: 8.8.8.8 , protocol: tcp , destination port: 443 at the INPUT chain was sent to target ACCEPT correctly

There is plenty more to do so get back to work

B,

Fig. 10.: The screen shot of successfully completed task in the game.

6.9 Cyber Awareness Challenge

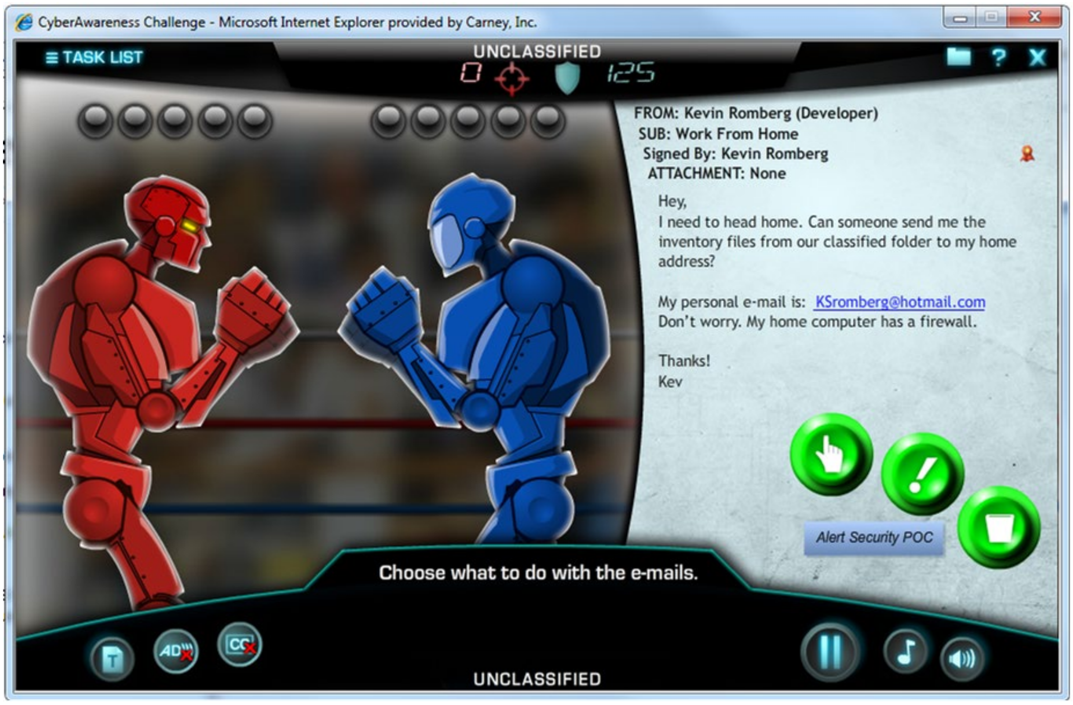
The Cybersecurity Awareness Challenge (CAC) presents cybersecurity and information systems security (ISS) awareness instructional topics through first-person simulations and mini-game challenges that allow the user to practice and review cybersecurity concepts in an interactive manner.

This game plays on the idea of going back to the future when a 2030 message is announced as an urgent warning of past security incidents that are seriously affecting life in the future. The user aims to prevent the occurrence of these incidents or to use evidence from files in the case the types of situations are not presented. Designed by the armed forces, the game promotes awareness of the scale of the impact of current incidents in the future. The goal is to lower the overall status of the threat and change the future. This game teaches information assurance practices that support the following objectives:

- Identify information assurance awareness/information systems security and why it is important

- Identify the different types of information and the requirements to protect each content type(for example, classified information, personally identifiable information, protected health information)
- Identify the different forms and methods of cyber-attacks (for example, social engineering, email phishing, viruses/malware, identity theft)
- Identify the types of technologies that are particularly vulnerable to attacks(for example, removable media, mobile computing devices –cell phones and tablets, wireless technology)

Goal or challenge of the game is to capture an unnamed hacker (referred to throughout the game as the “adversary”), who is targeting federal government information systems in order to access sensitive government information. To capture the adversary, players complete a series of tasks within the game that challenge them to engage in safe information assurance practices to protect government information systems and sensitive information.


CyberAwareness Challenge - Microsoft Internet Explorer provided by Carney, Inc.
≡ TASK LIST
UNCLASSIFIED
0
125
Alert Security POC
UNCLASSIFIED

FROM: Kevin Romberg (Developer)
SUB: Work From Home
Signed By: Kevin Romberg
ATTACHMENT: None

Hey,
I need to head home. Can someone send me the inventory files from our classified folder to my home address?

My personal e-mail is: KSromberg@hotmail.com
Don’t worry. My home computer has a firewall.

Thanks!
Kev

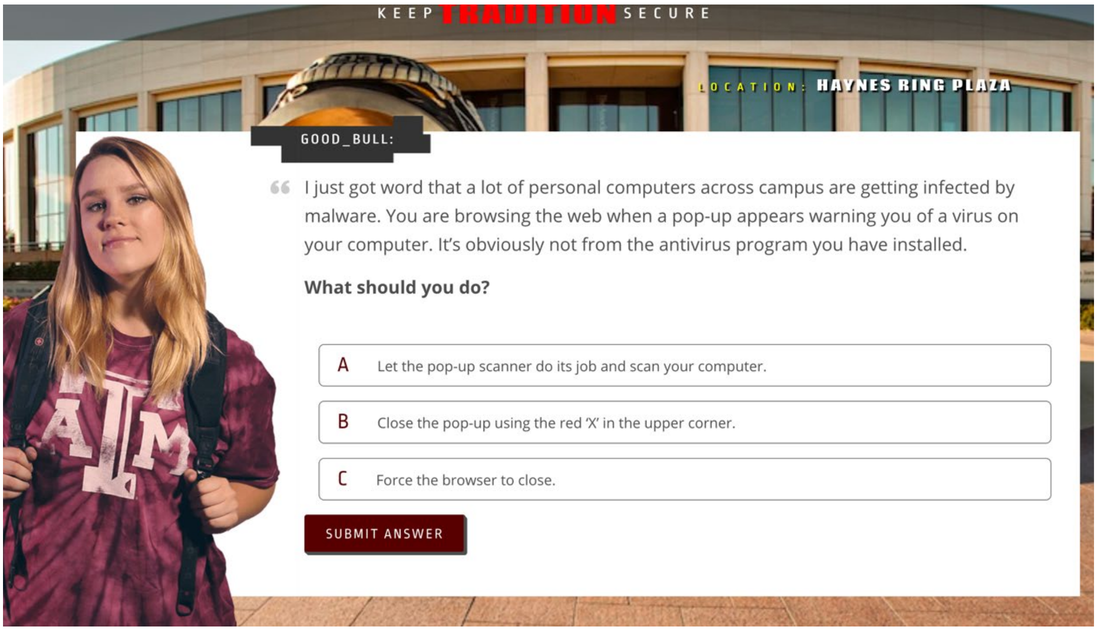
Choose what to do with the e-mails.

Fig. 11. : The Graphic User Interface of Cyber awareness Challenge.

6.10 Keep Tradition Secure

Keep tradition secure game (http://keeptraditionsecure.tamu.edu) is an on-line game that can be played anywhere using a laptop, desktop, tablet or mobile device. The game was developed by a researcher group of Texas in a A&M Texas University (Agricultural and Mechanical College of Texas). In the game, players help the hero known as “Good_Bull” to track a hacker, “Bad_Bull,” across the campus. Good_Bull needs your help. A notorious hacker with the screen name “Bad_Bull” hates Texas A&M tradition and is causing trouble around campus.

The principle of the game is more or less based on a quiz questions. Various questions about cyber security are presented and, when if answered correctly, the players get a clue intentionally left by the hacker in the form of riddles regarding Texas A&M traditions. The game is actually a good learning tool for basic cybersecurity knowledge. It is actually helping the user, to be aware on the everyday threats when browsing the internet. It is an asset that anyone can use, from young kids to older students or average internet users.



“ I just got word that a lot of personal computers across campus are getting infected by malware. You are browsing the web when a pop-up appears warning you of a virus on your computer. It's obviously not from the antivirus program you have installed.

What should you do?

A Let the pop-up scanner do its job and scan your computer.

B Close the pop-up using the red 'X' in the upper corner.

C Force the browser to close.

SUBMIT ANSWER

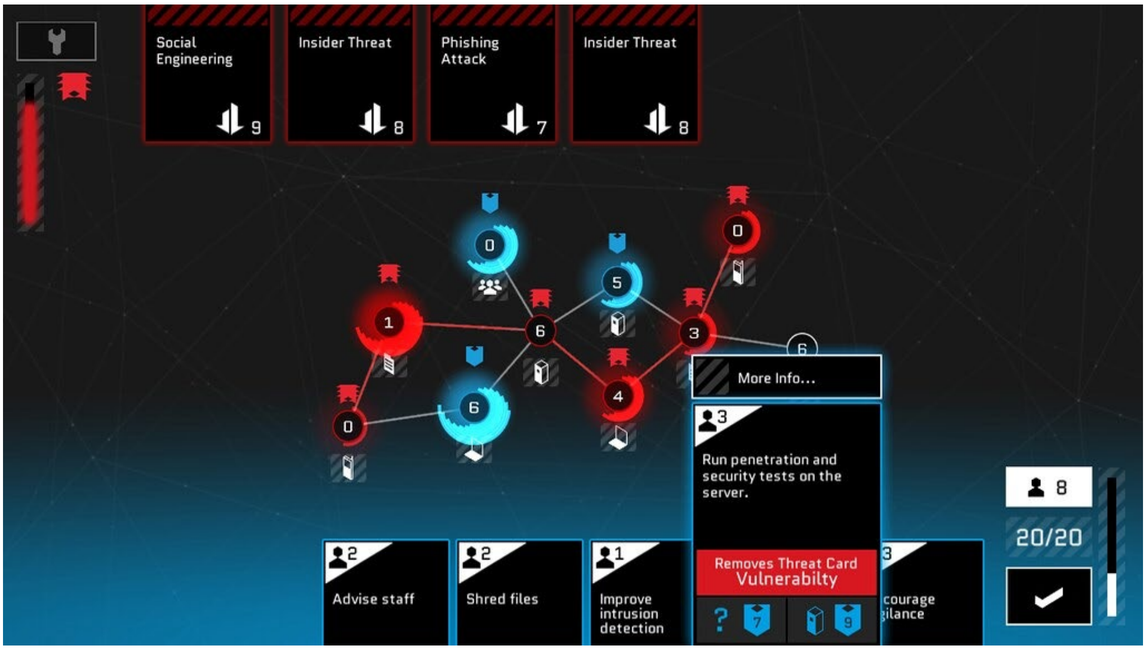
Fig. 12.: A screenshot of the Game: Keep Tradition Secure.

6.11. Zero Threat

Zero threat is cybersecurity training game, that targets employee complacency and goes beyond raising awareness to change learner behaviour. The game is using modern learning techniques such as 'learning by doing', and creating practice loops where learners can develop good habits in working in cybersecurity environments. The game especially is covering security topics such as phishing and vishing, password hygiene, mobile devices, the Internet of Thing and social media. The purpose of the game is to emotionally engage the learners by showing, rather than describing, the consequences of good and bad cyber-security decisions. While in nowadays in an increasingly digital workplace all over the world, the things can go wrong very quickly the approach taken in the game is up to date.
The game applies a »pull« rather than a »push« approach to training, inviting learners to replay and try to improve their score. The game have received a Silver award in the 2017 International Serious Play Awards a competition honouring outstanding digital games designed for education or training.
The game was developed by Governance, Risk and Compliance (short: GRC) training specialists Eukleia and learning game experts Preloaded, alongside learning and engagement specialists LEO.

Learners are placed in control of a network made up of both technology and people, full of valuable data which the learner must protect from a relentless onslaught of cyber-threats. These threats are based on real cyber-criminal tactics like social engineering and phishing. To stop them, the learner must ‘play’ countermeasures, and these too are closely based on the security measures employees need to be taking in real life.

Every action players can take in the game is associated with cyber-security good practice, and when threats hit, visual effects provide instant feedback. By integrating gameplay and learning, Zero Threat is able to keep learners playing and help them to build good cyber-security habits that are directly applicable in a day-to-day work environment.



Run penetration and security tests on the server.

6.12 Cyber Threat Game

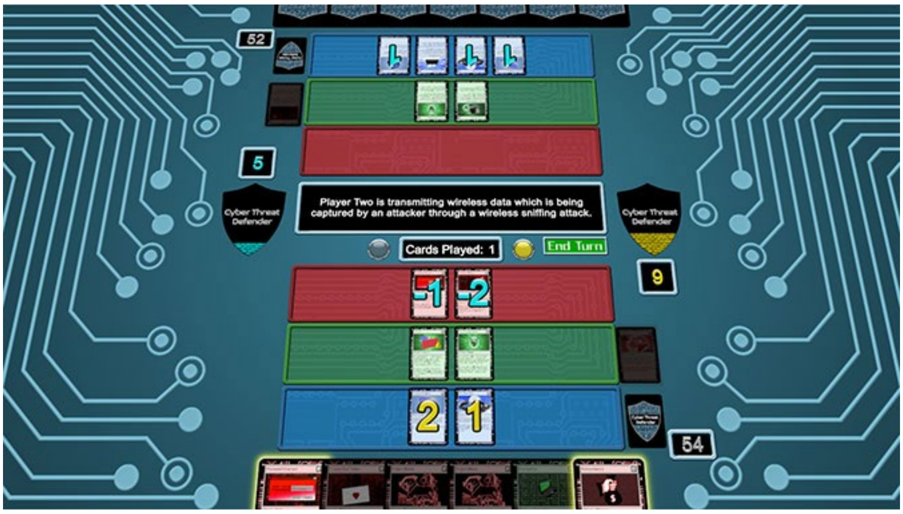
Cyber threat game was first launched in April 2016, as an extension of the Cyber Threat Defender game, which is a multi-player collectible card play game that is now available in an electronic card game format that can be download by the user. The PC version of CTD (Cyber Defender Game) was created by the Center for Infrastructure Assurance and Security (CIAS) at UTSA (The University of Texas at San Antonio), and it teaches players how to protect themselves from cyber-attacks while building robust networks. The game introduces students to basic cyber vocabulary and enable them to understand and reinforce the defence implementation. CIAS designs, builds and supplies the technology and the virtual machines for the CyberPatriot National Youth Cyber Defence Competitions and are also the creators of the Collegiate Cyber Défense Competition.

Cyber threat game is an easy-to-play, engaging game for any user regardless of the age or skill level. Players are supposed to protect themselves from attacks while building robust networks. The purpose if the game is to make exercises for a player intending to become a true Cyber Threat Defender. The objective of the game is to: introduce middle school students to basic cyber security vocabulary (available in English and Spanish), helping a high school students' to understand the defence implementation by providing a reinforcement in the professional training. Cyber threat game is a good complement to any curriculum of Science, technology, engineering, and mathematics (STEM) or any other cybersecurity curriculum.

To play the game, each player needs a deck of cards. With the cards, students build and protect their systems simultaneously. To begin the game, the players need to have two cards: desktop computer and ISP connection. After that, the player draw cards from his/her deck and begin building own assets, defences and attacking the opponent. This game is a fun game, but requires as well a strategy in the playing. The simplicity of the game enable kids, college students and professionals alike to play.

Apart from the starter deck, the game offers Booster packs. These Boosters introduce new concepts, add challenges and keep the gaming engagement fresh. The idea of teaching cybersecurity through a card game is still something that a lot of people question. Why would a game encompassing information from a highly technical field go “back in time” via a card game? The answer is simple, “because it works”.

When the game is set up, the player is able to see and understand the connection that each card has with each other.



Player Two is transmitting wireless data which is being captured by an attacker through a wireless sniffing attack.

Fig. 13.: A screenshot of digital version of a board Top-Table Game: Cyber Threat

7. Evaluation of the game properties

The CyberSecurity games classification and evaluation is worth to be approached. In the field of serious games have been in the past proposed many classification and taxonomy, the latest from Jerman Blažič (2017) . In this report the latest published classification was used. The elements that manage the classification are listed below.

7.1 Technical Properties:

Game Type: web-based/stand-alone
Distribution: Weather the game is free for use, played by licence, on CD-ROM, or run by downloaded application/client
Year of publishing: The year that game was become available for public use
Users: the number of registered users.
Label: The source, origin and the development team
Single/Multi user: Weather game can be played by one or requires more players
Dimension: Weather the game is present in 2D/3D environment
Genre: Table Top, Networking, Firewall, CTF, General

7.2 E-Learning properties/Learnability

Competitive or Non Competitive: If the game is based on the provision of correct decisions by the player or by the other participants (for example: Artificial Intelligence Players, such is BOT - an autonomous program)
Degree of complexity: what is the game decision input variable complexity, or how demanding is the computer model complexity
Feedback system: Weather the results are shown by presenting the players cores that has been reached during the game progress or by presenting the acquired experience points, the achieved upgrade level or the summary reports.
Deterministic or stochastic: The stochastic alternative or deterministic,
Background knowledge: basic/intermedia/advanced/professional knowledge or a beginner (general) knowledge required for playing the game.
Interactive type: In an interactive game participants respond to the questions at the computer, receive an immediate response, and then submit additional answers/decisions. In a non-interactive game decisions are submitted to the game administrator.

8. Table with the evaluated properties of the selected Cyber Security video games

For the purpose for this study, we have tested and played the presented games in chapter 5. The evaluation results are displayed in the following table:

	Target Attack	**Cybersecurity Lab**	**ThreatGen: Red Vs. Blue**	**CyberSIEGE**	**Permission Impossible**	**Data Center Attack**	**CS4G Netism**	**Firewall administration**	**Cyber Awareness Challenge**	**Keep Tradition Secure**	**Zero Threat**	**Cyber Threat Game**
TECHNICAL PROPERTIES												
Game type	Web Based	Web Based	Stand Alone	Stand Alone	Web Based	Web Based	Web Based	Web Based	Stand Alone	Web based	Web Based	Web Based
Distribution	Free	Free	Free	Free	Free	Free	Free	Free	For Academic users	Free	Free	Free
Year of publishing	2015	2020	2019	2004	2018	2017	2017	2017	2019	2018	2017	2016
Label	Trend Micro	NOVA labs	Derezzed	Naval postgraduate School	Sibylle Sehl	Trend Micro	Atwater and Bocovich	GitHub	LivingSecurity	Texas A&M	GRC	UTSA
Single/Multi user	Single	Single	Multiplayer	Single	Single	Single	Single	Single	Single	Single	Single	Multiplayer
Dimension 2D/3D	2D	2D	2D	3D	2D	2D	2D	2D	2D	2D	2D	2D
Genre	General	General	Catrure The Flag	Network	Firewall	Network	Network	Firewall	General	General	Network	General
E-LEARNING PROPERTIES/LEARNABILITY												
Competitive/Non Competitive	Competitive	Non Competitive	Competitive	Competitive	Non competitive	Non competitive	Non Competitive	Competitive	Competitive	Non Competitive	Non Competitive	Competitive
Degree of complexity	Low	Medium	Low	Low	Medium	Medium	Low	High	Low	Low	Medium	Medium
Feedback system	Score points	Level Score	Score points	Level upgrade	Level upgrade	Level upgrade	Score points	Score points	Level upgrade	Level upgrade	Level upgrade	Level upgrade
Deterministic/stochastic	Stochastic	Stochastic	Deterministic	Stochastic	Stochastic	Deterministic	Stochastic	Deterministic	Deterministic	Deterministic	Deterministic	Deterministic
Background knowledge	Basic	Intermedia	Advanced	Advanced	Intermedia	Intermedia	Advanced	Advanced	Basic	Basic	Intermedia	Intermedia

Interactive type	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	No

Table 1.: The Evaluation and Classification of Selected CyberSecurity Games.

9. Comments and discussion

Overall, the available Cybersecurity games on the web belong to different types or categories, due to variety of »learning« content that can be »digest« in order to make the student`s skills well trained. The group where a cybersecurity game is allocated depends on the purpose of the usage and the achieved goals in the educational process. Unfortunately, by playing few cybersecurity games that have been selected out from the current stage of »world of cybersecurity games« it was not possible to cover the training needs of the overall cybersecurity field, due to its complexity and diversity. Many topics are missing for example organizational and human behaviour security aspects. However, some insight from the cybersecurity addressed topics was possible to be elicited with the existing games that differ as well regarding the levels, from the beginner to advanced expert trainee. Another finding is that there is no sufficient game that could »train« the whole existing CyberSecurity levels or topics. However, this study report has shown that, different games can provide different skills and practice. By deciding/selecting the “filed” of cybersecurity that need to be “trained” with support of particular game, the most appropriate game for the required training can be still found as the selection of cybersecurity games is currently much large and rich compared with the past. By reviewing several games that are presented in this report, it was found as well that limitations still exist as the games do not support all needed educational aims, educator`s objectives and planned outcomes. Some games have very high level of design is the designers intended to fulfil the learning methods, but some games are very poor and do not meet the requirements that are expected to bring the learning purpose out.

However, when selecting the most adequate CyberSecurity game, it is important to know that the game scenario must be to be enjoyable and has to be »embedded« within a great story-line to meet the educators or learners expectations. At this point it is important to notice that such games have high fragments or level of reality. The better the reality imitation in the game is, the learner outcomes are more valuable. Games that designed to be very close to the reality enable faster transfer the knowledge and the experiences is more directly passed to the players which results in better achievement of the learning target. For example, some games such is The DATA ATTACK are good example, as they offer pre-recorded real videos and dialogue scenes, giving a good in-sight to the learners how to deal with cybersecurity issues. Such games enable effective way to teach students how to act and adopt the right decisions in the cybersecurity field. Students are usually instructed how to use the game scenarios and with the scenarios close to reality they are far more likely to retain what they have learned, compared to those students taught by use of traditional lectures and case-study methods. On the other hand, the game The Firewall administration is designed with low design scenario and story-telling, and low attractive graphic environment and simplicity of use. Due to these characteristics it can provoke a real monotonous practice and become less compared to the interesting and close to reality-scenario concept.

10. Conclusion

Cyber security as an area consists of a number of different aspects, from digital equipment, software and cryptography to human processes and psychology. Training of cyber security using serious games is a young and developing field. The training is based on a complex strategy game set in a virtual cyber-world with attempts to resemble to the reality. The games range from actionable to educational classroom activity with intention to spur conversation. The report presented in this paper has identified, that despite some deficiency the games in the area of cybersecurity provide better training of both the general public, industry and businesses compared with education without gaming. A number of games have been developed, academic studies have been conducted that include an evaluation of the effectiveness of the game for education and training. The results from these studies are generally positive, however the sample sizes are still small and no effect of the sample size have been mentioned in the studies. It is clear that more robust evaluations with sizeable samples are needed, in order the educators and the trainers to be able to conclude more detailed with data supported findings on the effectiveness of serious games for cyber security education and training. Most of interventions found in the field were mainly focused on the game development that can be finished over a relatively short period and in just one session. This is surprising considering that these games do not just aim to inform, but their ultimately should aim to change the player's long-term security behaviour. It is also interesting to note that all but one of the interventions evaluated targeted home computer users or the general public.

Serious games have been treated nowadays in the light of good and protentional successful learning and training tool, yet the field of CyberSecurity gaming needs still much more to discover for becoming regular educational tool. For this area it is important that the serious games to behave like a model that imitate the real-life situation in order they to be successful the CyberSecurity students/learners to take them and train themselves before they step a foot in the real world environment. CyberSecurity educational curriculum is different, compared to other educational fields, such are those from the field of Science, technology, engineering, economics and mathematics, as they have the contents that can be simulating with the 3D graphics and virtual environment, where users can interact with elements such are avatars and similar items. On the other hand, CyberSecurity is a type of science where the learners can only interact with a computers build in the virtual environment. This finding is important for provision of the CyberSecurity games for training and learning tool usability to meet the expectation of the two main groups of learners: IT professionals and management decision makers. In that context It is worth considering the need for building the bridge between CyberSecurity experts and the educator expertise for fruitful »coexistence« in the design of the next generation of games for CyberSecurity. At this point it is important also, how to plan and re-write the game scenario in order to motivate a learner to be involved into the game-flow to reach the main goal of every educational game: learning by playing.

11. References

Arachchilage N. A. G and Asanka N. (2012), “Security awareness of computer users: A game based learning approach,” Brunel University, School of Information Systems, Computing and Mathematics, 2012.

Arachchilage N. A. G. and Love S., (2013)“A game design framework for avoiding phishing attacks,” Comput. Hum. Behav., vol. 29, no. 3, pp. 706–714, 2013.

Arnab, S., Dunwell, I. , Debattista, K. (2013). Global, *Serious games for healthcare: Applications and implications*. Medical Information Science Reference, 2013.

Arachchilage N. A. G. and Love S (2014)., “Security awareness of computer users: A phishing threat avoidance perspective,” Comput. Hum. Behav., vol. 38, pp. 304–312, 2014

Arachchilage N. A. G. and Love S., (2018) “A game design framework for avoiding phishing attacks,” Comput. Hum. Behav., vol. 29, no. 3, pp. 706–714, 2013. http://dx.doi.org/10.1016/j.chb.2012.12.018

Arnab S., Dunwell I., Debattista K., and Global I. G. I., (2013) Serious games for healthcare: Applications and implication. Medical Information Science Reference, 2013. http://dx.doi.org/10.4018/978-1-4666-1903-6

Atwater E., Bocovich C., Hengartner U., and Goldberg I. (2017) Netsim: Network simulation and hacking for high schoolers, 2017 {USENIX} Workshop on Advances in Security Education ({ASE} 17)

Borret M. (2014): eBook: How To Stay Ahead in the Cybersecurity Game, Security Intelligence

Chou, C. & Peng, H. (2011), "Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience", The Internet and Higher Education, vol. 14, no. 1, pp. 44-53.

Cauberghe V. and Pelsmacker, P. De (2010)“Advergames,” J. Advert., vol. 39, no. 1, pp. 5–18, 2010.

Cugelman, B. (2013) “Gamification: What It Is and Why It Matters to Digital Health Behavior Change Developers,” *JMIR Serious Games*, vol. 1, no. 1, p. e3, Dec. 2013.

Cone B. D., Thompson M. F., C. E. Irvine, and T. D. Nguyen, Cyber Security Training and Awareness Through Game Play. Springer, 2006. http://dx.doi.org/10.1007/0-387-33406-8_37

Cauberghe V. and De Pelsmacker P., (2010) “Advergames,” J. Advert., vol. 39, no. 1, pp. 5–18, 2010. http://dx.doi.org/10.2753/JOA0091-3367390101

Compte Le, A. D. Elizondo and T. Watson, (2015)"A renewed approach to serious games for cyber security," 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, Tallinn, 2015, pp. 203-216, doi: 10.1109/CYCON.2015.7158478.

Cheswick W. R., S. M. Bellovin, and A. D. Rubin. (2013) Firewalls and Internet security: repelling the wily hacker. Addison-Wesley Longman Publishing Co., Inc., 2003

Dunwell, I. , Petridis, P. S. Arnab, S. de Freitas, P. Lameras, C. Stewart, and M. Hendrix, (2014)“A Game-Based Learning Approach to Road Safety: The Code of Everand,” in CHI’14: Proceedings of the 2014 CHI Conference on Human Factors in Computing Systems, 2014.

Eriksson, H. , Kovordányi, R. and Rankin, A. (2010)"CRISIS–Virtual-Reality-Based Training for Emergency Management," presented at the First National Symposium on Technology and Methodology for Security and Crisis Management (TAMSEC), Linköping, Sweden, 2010.

Flin R. H. and Arbuthnot, K. (2001) Incident command: Tales from the hot seat. Ashgate Pub Limited, 2002.

Gonzales, H. F., Llamas-Contreras R., Ordaz D., (2017) Cybersecurity Teaching through Gamification: Aligning Training Resources to our Syllabus. Research in Computing Science 2017 146(1):35-43 DOI: 10.13053/rcs-146-1-4

Gondree, Mark A. et al. (2016). "Talking about Talking about Cybersecurity Games." login Usenix Mag. 41 (2016): n. pag.

Hendrix, Maurice & Al-Sherbaz, Ali & Bloom, Victoria. (2016). Game Based Cyber Security Training: are Serious Games suitable for cyber security training?. International Journal of Serious Games. 3(1). 10.17083/ijsg.v3i1.107

Labuschange, W.A.,, Eloff, M.M. (2014) "The dark side of Web 2.0" 13th European Conference on Cyber Warfare and Security (ECCWS 2014), Piraeus, Greece, 3-4 July 2014

Labuschagne, William Aubrey; Eloff, Mariki,(2019): "The Effectiveness of Online Gaming as Part of a Security Awareness Program." 18th European Conference on Cyber Warfare and Security: wargaming papers (ECCWS 2019), Portugal, Coimbra 4-5 July, 2019.

Pastor V., Díaz G., and Castro M., (2010) "State-of-the-art simulation systems for information security education, training and awareness," in Education Engineering (EDUCON), 2010 IEEE, 2010, pp. 1907–1916.

Richard A. (2014) "'Education in Disguise': Culture of a Hacker and Maker Space," InterActions: UCLA Journal of Education and Information Studies, vol. 10, no. 1, 2014.

Sehl, Sibylle & Vaniea, Kami. (2018). Permission Impossible: Teaching Firewall Configuration in a Game Environment. 10.14722/eurousec.2018.23006.

Sehl S., Vaniea K (2018); In European Workshop on Usable Security (USEC). 2018.

VanOmmeren E., Borrett M., Kuivenhoven M., (2014). Staying ahead in the Cyber Security Game. Sogeti., IBM.

Karspersky. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (Last Access: 5.4. 2020).

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

Thompson, (2011). Active Learning with the CyberSIEGE game, (2011)