EPiC Series in Computing

Volume 93, 2023, Pages 129–140

Proceedings of Society 5.0 Conference 2023

A Cyberattack Simulation for Teaching Cybersecurity

Christopher Scherb[1] [*], Luc Bryan Heitz[1][†], Frank Grimberg[1][‡], Hermann Grieder[1][§], and Marcel Maurer[2][¶]

[1] University of Applied Sciences and Arts, Northwestern Switzerland, Basel, BS, Switzerland
christopher.scherb@fhnw.ch
luc.heitz@fhnw.ch
frank.grimberg@fhnw.ch
hermann.grieder@fhnw.ch
[2] Muuri Solutions, Bern, BE, Switzerland
info@muuri.solutions

Abstract

With the rising number of cyberattacks, such as ransomware attacks and cyber espionage, educating non-cybersecurity professionals to recognize threats has become more important than ever before. However, traditional training methods, such as phishing awareness campaigns, training videos and assessments have proven to be less effective over time. Therefore, it is time to rethink the approach on how to train cyber awareness. In this paper we suggest an alternative approach – a serious game – to educate awareness for common cyberattacks. While many serious games for cybersecurity education exist, all follow a very similar approach: showing people the effects of a cyber attack on their own system or company network. For example, one of the main tasks in these games is to sort out phishing mails. We developed and evaluated a new type of cybersecurity game: an attack simulator, which shows the entire setting from a different perspective. Instead of sorting out phishing mails the players should write phishing mails to trick potential victims and use other forms of cyberattacks. Our game explains the intention of each attack and shows the consequences of a successful attack. This way, we hope, players will get a better understanding on how to detect cyberattacks.

Keywords— Cyber Security, Serious Game, Education, Awareness, Phishing

1 Introduction

The past few years have seen a significant rise in the number of cyber attacks across the world. With the increased digitization of business processes, home automation [12], connected cities [13]

[*] Idea and Supervision of Development, Implementation and Evaluation
[†] Background Research, Study Design, Evaluation
[‡] Proofreading and Feedback
[§] Supporting design of the User Study
[¶] Design, Development and Implementation of the Serious Game during his Master Thesis

and the rise of remote work, cyber criminals have found new and sophisticated ways to exploit vulnerabilities in computer networks, computer systems and humans. From phishing scams and ransomware attacks to data breaches and identity theft, cyber attacks have become a major concern for businesses, governments, and individuals alike. The COVID-19 pandemic has also further exacerbated the problem, with cyber criminals taking advantage of the increased online activity to launch targeted attacks on vulnerable individuals and organizations. As technology continues to advance, the threat of cyber attacks is likely to grow, making it imperative for individuals and organizations to stay vigilant and take proactive measures to protect themselves from these digital threats.

Meanwhile, the portrayal of hacking in popular media such as in the series *NCIS*[1] and the video game *Watch Dogs*[2] is often dramatized and unrealistic. In these shows and games, hacking is often depicted as a glamorous and effortless activity, where hackers can break into highly secure systems with just a few keystrokes. While these shows and games may be entertaining, they can perpetuate the misconception that hacking is a harmless activity, leading to an inadequate awareness about the risks associated with cybersecurity. In reality, hacking is a complex and often illegal activity that can result in serious consequences for both the hacker and victim. As the negative impact of hacking, including identity theft, financial fraud, and disruption of critical infrastructure is often inaccurately represented by the media, the media does portray a sense of helplessness once one becomes the target of a hacker. Yet, most attacks could have been avoided by most non-technical employees if they had good security awareness education.

Therefore, one of the most important ways to mitigate the risk of cyberattacks is by educating employees on best practices for cybersecurity [10, 17]. Employees are often the first line of defense against cyber threats, and without proper training, they may inadvertently expose their company's sensitive information or fall prey to phishing scams [4]. By providing comprehensive cybersecurity training to employees, businesses can empower them to identify and report suspicious activities, secure their devices and accounts, and adhere to best practices for data protection. This can help prevent costly data breaches and cyber attacks, and also foster a culture of security awareness across the organization. In short, investing in employee cybersecurity education is a crucial step towards safeguarding a company's valuable assets and reputation in today's digital landscape.

However, educating cybersecurity is a quite complex topic and most employees consider training and awareness campaigns as annoying and participate halfhearted. Moreover, recent research has shown, that awareness training such as phishing campaigns have only a short term effect [8] and do not increase the employees resistance to phishing mails in long term. One reason for this is that phishing emails have become increasingly sophisticated, making them more difficult to detect. Attackers use tactics such as social engineering, spoofing legitimate email addresses, and creating convincing fake websites to trick unsuspecting victims. Additionally, some employees may not take phishing threats seriously or may be too busy to fully scrutinize every email they receive. Even with training and awareness programs, employees still may fall for phishing mails. Further, phishing awareness campaigns itself can contribute to naive behavior of employees as dealing with mails from phishing awareness campaigns may not inflict any harm when clicking on arbitrary links. As such, the underestimation of the phishing-related risk may be habituated, making real phishing mails even more critical.

By understanding the tactics used by attackers, such as social engineering and spear-phishing, individuals can be better equipped to recognize and avoid phishing attempts. Additionally,

[1] https://www.imdb.com/title/tt0364845/
[2] https://www.ubisoft.com/en-us/game/watch-dogs/watch-dogs

appreciation of the potential consequences of falling victim to phishing can motivate individuals to take the necessary precautions to protect their sensitive information. Many people do not understand what harm clicking on an email or clicking on a link can cause not only to their system but to the entire network, since they have never seen the consequences such as systems encrypted by ransomware, stolen company secrets or financial fraud.

Therefore, we designed a cybersecurity education game, in which the player experiences cyber attacks from the attacking side [9]. The player plays an attacker, who needs to acquire information, sends phishing mails, uses exploits and other forms of cyber attacks to attack a company [14]. The process is presented as realistic as possible. The user has to search for email addresses of victims, fake websites for phishing attacks and buy exploits in a simulated darknet store. The consequences of each attack are shown and explained, so that the player can develop an deeper understanding of the motivation and the different shapes of cyber attacks and by this the resistance against real cyber attacks.

In the upcoming sections of this paper we will detail our game as follows: Section 2 contains reviews of literature that introduce the reader to the setting and which contain background knowledge for this paper. Section 4 gives an outline of our serious game as a whole and in more detail for each implemented scenario. The results of a short term survey are presented and discussed in Section 5. In Section 6 we conclude this paper and highlight potential future work.

2 Literature Review

In this section we present and summarize related and background work.

2.1 ENISA Threat Landscape Report

The ENISA Threat Report[3] is an annual publication by the European Union Agency for Cybersecurity (ENISA). The report provides an overview of the current state of cybersecurity threats and trends in Europe, as well as globally. It analyzes the most significant cybersecurity incidents that occurred during the previous year and identifies emerging threats and vulnerabilities that could impact individuals, organizations, and critical infrastructure.

The report also includes recommendations for improving cybersecurity such as best practices for risk management and incident response. It is intended for a broad audience, including policymakers, IT professionals, and the general public, to increase awareness of the current cybersecurity landscape and help stakeholders make informed decisions about how to protect their digital assets.

The ENISA Threat Report is an important resource for anyone interested in understanding the current state of cybersecurity and how to mitigate potential risks and is beneficial to establish which important skills are required to mitigate the exposure of cyberattacks.

2.2 NIST Cybersecurity Framework

The NIST Cybersecurity Framework [16] is a set of guidelines, standards and best practices developed by the National Institute of Standards and Technology (NIST) to help organizations manage and reduce cybersecurity risks. The framework consists of five core functions: Identify, Protect, Detect, Respond, and Recover. Each function contains a set of categories and subcategories that provide detailed guidance on specific actions that organizations can

[3] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

take to enhance their cybersecurity posture. The framework is widely recognized and used by government agencies, private companies, and organizations of all sizes to improve their cybersecurity practices and mitigate the risk of cyberthreats.

The framework was first released by NIST in 2014, and it has since been widely adopted by organizations in various industries, including healthcare, finance, and energy. It is designed to be flexible and adaptable to the unique needs and risk profiles of each organization, regardless of size or sector.

The five core functions of the framework are as follows:

- Identify: This function involves developing an understanding of the organization's systems, assets, data, and risks. It includes activities such as inventorying hardware and software assets, identifying vulnerabilities and threats, and assessing the potential impact of cybersecurity incidents.
- Protect: This function focuses on implementing safeguards to protect against cyber threats. It includes activities such as access control, data encryption, and security awareness training for employees.
- Detect: This function involves identifying cybersecurity incidents as quickly as possible. It includes activities such as continuous monitoring, anomaly detection, and incident response planning.
- Respond: This function involves taking immediate action to contain and mitigate the effects of cybersecurity incidents. It includes activities such as incident response, business continuity planning, and disaster recovery.
- Recover: This function involves restoring normal operations after a cybersecurity incident. It includes activities such as system recovery, damage assessment, and post-incident review.

From the NIST Cybersecurity Framework a list of skills which are essential for a better protection from cyber risks, for both developers and general users of computer systems can be derived [5]:

- Preventing malware via non-trustworthy websites
- Preventing malware via email phishing
- Preventing Personal Identifiable Information theft via access to non-trustworthy websites
- Preventing Personal Identifiable Information theft via email phishing
- Preventing Personal Identifiable Information via social media
- Preventing information system compromise via USB or storage device exploitation
- Preventing unauthorized information system access via password exploitation

The framework is intended to be used as a tool for improving an organization's cybersecurity practices, rather than as a one-size-fits-all solution. It is a living document that can be updated and customized over time to reflect changes in technology, threats, and business needs.

2.3 Phishing in Organizations: Findings from a Large-Scale and Long-Term Study

The research project *Phishing in Organizations: Findings from a Large-Scale and Long-Term Study* [8] ran a large scale experiment in a company where more than 14'000 employees participated. The goals were to understand if certain employees are likelier to fall for phishing than others, how the overall vulnerability to phishing of the company evolves over time, how effective phishing warning and training is and how effectively crowd-sourced phishing detection is applied in companies. The study confirms previous findings that both age and computer skills correlate with being susceptible to phishing. Further it was revealed that the most vulnerable employees were those that use computers daily for repetitive tasks using specialized software only. A more concerning finding of the study was that simulated phishing exercises and voluntary training did not just fail to improve resilience but, rather contradictory, made them more prone to fall for phishing attacks. The severity of this finding is even worse when combined with the observation that a longer exposure to phishing attacks may lead to a higher portion of employees being susceptible for it. On the positive side it was demonstrated that crowd-sourced phishing detection can be efficient in large organizations.

2.4 Cyber Security Training A Survey of Serious Games in Cyber Security

In the paper *Cyber security training a survey of serious games in cyber security* [21] a survey of academic and non academic serious games that focus on cybersecurity was conducted. The study emphasizes that while a lot of effort has been put into technical security, drastically less attention has been put into how to better educate users, which are considered to be the weakest link in the security chain. It is further stated that effective large scale measures rather target a technical audience while little is done to overcome the perception that cybersecurity is for tech savvy people only. Compared to hands on training methods game based learning allows students, or even encourages, to make mistakes in a risk-free environment and learn from them [15]. Further it is argued that well designed serious games can retain all advantages of traditional and hands-on training while remaining low-cost. Based on the survey it is concluded that serious games for cybersecurity seem promising but there is a lack of proper evaluation of these games and therefore no conclusive answer on the effectiveness can be given.

3 Research Design

The goal of our cyberattack simulator is to improve the knowledge about cyberattacks in the general society. Therefore, we designed a study to question players of our game before and after playing to understand the impact of the game on the knowledge about cyberattacks. The related questionnaire is organized in a structured form, so asking either *yes or no* or range questions with a range from one to five. The questions have a main focus on the phishing part of the game, since we assume that most people have been in some contact with phishing [3]. We distributed our questionnaire to bachelor students of two different research institutes as well as to further people randomly. The first survey before the game focused on the existing knowledge of the participants in the field of cyberattacks. The second survey after the game verified whether the knowledge about cyberattacks improved by playing the game, thus it consists of almost completely the same questions. The surveys were done anonymously, and we did not track the answers of individual participants from before and after the game. We received 32

answers pre game and 15 answers post game. Our study only analyzed the short term effects, as we did not perform any assessment a longer period after playing the game (e.g., half a year or a year later).

4 Game Design

In this section we describe the game design of our cyberattack simulator. We focus on the most important part of the game – the scenarios. Later, we will discuss the actual game design such as the graphics and style.

The central goal of the game is to give the players, regardless of their technical knowledge, a better understanding on how cyber criminals perform cyberattacks and how they approach targets by letting them perform the attacks themselves. Attack centric games are not uncommon to teach cyber security skills and are often encountered in the form of Capture the Flag (CTF) games. The drawback is that they usually either require extensive technical knowledge or time to play. Our serious game approach aims to make cybersecurity games more accessible to a wider audience and allow them to explore freely, without having to fear making mistakes. The game is divided into different scenarios, each corresponding to real world attacks that bad actors use. By interacting with the character *Nate* the player can choose which scenario to play first. After choosing a scenario the player moves their character to a computer in the game from which the chosen attack is launched. The following subsections will first provide a mapping from the NIST framework to our scenarios and then introduce and explain the currently available scenarios for players to explore.

4.1 Mapping Cybersecurity Skills to Game Scenarios

We used the NIST framework (see section 2.2) as basis for our scenarios and summarizing the different skills required to successfully face cyberattacks into four categories.

We start by summarizing the skills into categories.

1. The first scenarios is add *Phishing/Social Engineering* where the skills *Preventing malware via email phishing*, *Preventing Personal Identifiable Information theft via email phishing*, *Preventing Personal Identifiable Information theft via access to non-trustworthy websites* and *Preventing Personal Identifiable Information via social media* are covered. The scenario will walk a player through a typical phishing attack to understand the way an attacker thinks and to educate them on the concepts they should recognize in phishing mails.

2. The second category is more of a category for developers. It covers the *Preventing unauthorized information system access via password exploitation* skill. The scenario walks the player through a situation where an attacker can steal information from a non secure website.

3. The third category is about Metasploit [7], which is an attack framework for penetration testing but could also can be abused by attackers, and covers the importance of patching and updating critical systems. This is also a more developer and system engineer focused scenario and relies on recommendations from the ENISA thread landscape (see section 2.1) and covers the skill *Preventing malware via non-trustworthy websites.*

4. The fourth and last category is about *bad USB keys.* It covers the skill *Preventing information system compromise via USB or storage device exploitation* and walks the

player through how attackers could obtain malware from the darknet and use USB keys to find a way into a company network.

For each category a scenario is created. In the following section all scenarios are described in more detail. Currently, the scenarios are sample scenarios we created based on the information from the NIST framework and the ENISA threat landscape to cover and evaluate the base skills. In the future more scenarios will be developed to cover more advance attack scenarios.

4.2 Social Engineering and Phishing

The term social engineering describes the act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust.[4] In order to convince victims to provide information or services social engineers rely heavily on the six principles of influence [23]. Based on these principles social engineers use the following with slight adaptions: authority, intimidation, consensus/social proof, scarcity, urgency and familiarity/liking. Commonly the attacker engages the target over email which is known as phishing in the general case and spear-phishing if it is targeted to a specific organization or individual. The Verizon Data Breach Investigations Report [5] states that more than 60% of the breaches in Europe, the Middle East and Africa included a social engineering component and despite awareness campaigns and exercises many still fall for phishing mails. Social engineering is the most common entry point for attackers and the easiest to avoid if employees are properly educated. Further it requires very little technical knowledge to defend against phishing and therefore anyone can and must be properly trained against it.

In our game the player begins the social engineering attack by using social media in order to gather information about the target. After finding a business email address on social media the player proceeds to check if the email has been part of a known data breach where passwords have been leaked. As the email has not been part of a leak the player receives the option to start a phishing attack. The game proceeds to guide the player step by step through a simplified but real phishing attack using SocialPhish[6]. More complicated commands and searches are replaced through clicks and specific text inputs to be more user friendly. In order to get the login credentials of a target the game makes use of the principle of urgency by sending a fake email from Facebook that tells the target that his account is about to expire. The target falls for the phishing email and the phished credentials are displayed on the screen.

4.3 SQL Injection

In 2021 Injection based attacks were placed third in OWASP's Top 10 ranking [2], a standard awareness document for developers describing the Top 10 web application security risks. In the previous ranking of 2017 Injections were first place. SQL Injections are a particular type of an injection based attack where databases are targeted. By injecting SQL statements into input data an attacker tries to manipulate the queries such that sensitive data is manipulated or revealed. Further consequences of a successful attack are executing administrator commands in the Database Management System, try to steal content of files present in the database and in some cases even to execute commands on the underlying operating system. Software is

[4] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
[5] https://www.verizon.com/business/resources/reports/dbir/
[6] https://github.com/xHak9x/SocialPhish

susceptible to SQL Injections if it interacts with an SQL database, takes data from an untrusted source, such as user input on a website, and dynamically uses that data to construct queries [6].

As this is a more technical and advanced concept our game only briefly introduces the concept of SQL Injections by walking the player through an attack and explaining the underlying concepts. The Injection allows the player to bypass a login and access the test server in order to search through the files. By looking into the various folders (and based on their contents) possible follow up actions, as well as their intentions, are explained.

4.4 Metasploit

The Metasploit Framework [16] is a tool for creating and executing exploits against targeted machines. At its core it is a collection of known vulnerabilities and payloads that is meant to help penetration testers to better test systems and always having an up to date catalog of attack options. When performing an attack with the framework it supplies a skeletons of known exploits and lets the user manually set specific targets and options. Further the framework provides Meterpreter, a payload that allows to take over control of the victims system. Both the Metasploit Framework and Meterpreter are publicly available and therefore not only used by security experts to attack systems in a legal manner but also by attackers performing illegal actions.

The scenario begins with the player executing a network scan using the tool Nmap [1], a popular security scanner that scans networks for hosts and which services are running on them. After performing the initial scan the player is then guided through the typical setup of an exploit in the Metasploit Framework and its configuration to attack a specific target with a selected payload. After typing *run* the exploit executes successfully and a Meterpreter session is started on the targeted device. This session is then used to find and download sensitive data. The scenario ends with a note that at this point the system is severely exposed and that an attacker can now perform various malicious actions, e.g., the installing of malware on the targeted host.

4.5 Bad USB

Bad USB also known under the name of Rubber Ducky, a bad USB manufactured by Hak5[7], is an attack where modified USB sticks are used to attack systems. These USB sticks usually contain additional programmable microcontroller that allow the attacker to program it [22]. Once plugged into a system the bad USB emulates a keyboard and is directly recognized from the targeted system as such. The device then initiates keystrokes and issues commands to the targeted system. Such commands can be opening a terminal and downloading ransomware, find and steal sensitive data or harmlessly prank users by turning the targeted system off. In order to be successful the attacker only needs to plug in the USB into the target system or convince someone else to do so. There are also large fashion attacks where attackers send USB devices as gifts to employees of a targeted company. By sending bad USB's to hundreds of employees there is a high chance that one of them will use it in the near future on a company device, giving the attacker an entry point to further attack the target [11].

To be able to start this scenario the player first needs to find the USB stick placed on a desk in the room. The game then explains how a bad USB attack works and gives the player a choice on how to proceed. The first option is to flash it with a Zero Day vulnerability, a vulnerability that is yet not known to the producers of software. The game illustrates how

[7] https://shop.hak5.org/

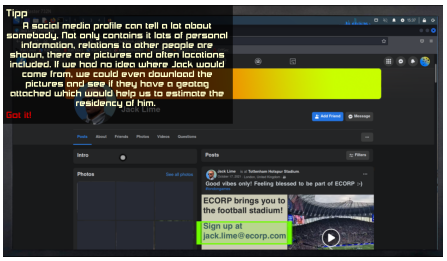

Figure 1: Screenshot of the implemented phishing scenario.

cyber criminals can get hold of such vulnerabilities by guiding the player to the darknet to purchase such an exploit. It also explains how cyber criminals remain anonymous while using online black markets. After purchasing the Zero Day the scenario ends in letting the player choose how to label the USB stick with a wording that would motivate employees finding it to plug it in into their computer.

The second option is less malicious and includes a batch script that opens Microsoft Word 5 times. It is further explained that this script can be linked to an image in order to increase the likelihood that someone accidentally executes it. While in this scenario a harmless example is used, the script is interchangeable and can contain far more malicious contents. This option ends in the player proceeding to take the aforementioned Zero Day option.

4.6 Game Implementation

The design of the game has been influenced by Cybersiege [18, 19, 20] which led to the design of a small narrative that is followed by different scenarios showcasing real cyberattacks. The game is 3D which allows the player to walk freely around the room and explore it. It has been developed by using Adventure Creator[8], a plugin for the Unity[9] game engine that allows to develop games with visual scripting. When the player interacts with the in-game-computer the scene switches to a pseudo 2D environment only showing the screen. In order to be able to run in a browser with WebGL the game was heavily compressed to a size of 190MB. Figure 1 shows a screenshot of the phishing scenario in the game where the game informs the player about the potential risks of posting sensitive information on social media.

5 Evaluation

In order to evaluate our game we conducted a short term survey (see section 3) where the participants were asked to fill out a form before and after the game. As usual with pre and post surveys we received more pre than post results. We did not opt to add personal identifiers to each form in order to preserve the privacy of the participants. This made it impossible to link pregame forms to postgame forms. In figure 2 we see that almost all participants knew what a phishing mail is.

But as seen in figure 3 most of the participants had little to no knowledge on how a phishing attack is rolled out before playing our game. In the post game results we can see a clear improvement of the understanding on how a phishing attack is rolled out. Despite the

[8] https://adventurecreator.org/
[9] https://unity.com

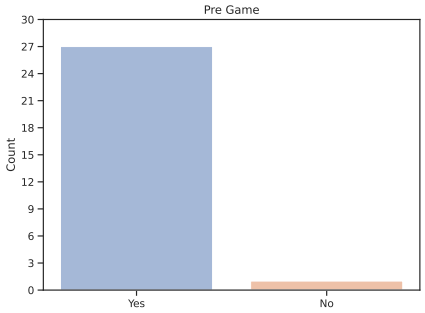

Figure 2: Answers to the question: Do you know what a phishing mail is?

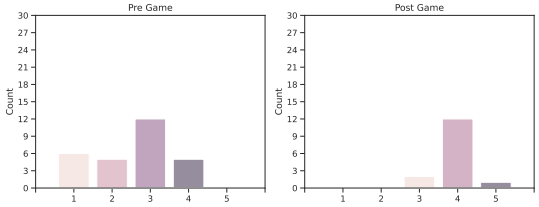

Figure 3: Answers to the question: Do you know how a phishing attack is rolled out?

imbalance of pre and post results we conclude from the absolute numbers that the participants gained a better understanding from playing our game. As shown in figure 4, we also asked the participants if they know how phishing attackers can acquire their email. Also here the awareness on how attackers can acquire emails of victims increased. At the end of the survey we asked the participants whether they in general learned more about cyber attacks and risks through our game. From figure 5 it can be concluded, that on average, the game has led to an improved understanding of cyber attacks and cyberrisks for the players of the game.

6 Conclusion & Future Work

In this paper we highlighted common cyber threats for employees in their day to day business and the related potential consequences. Further we emphasized that for phishing and social

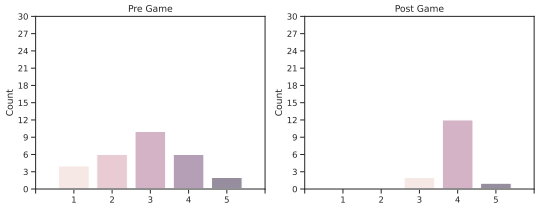

Figure 4: Answers to the question: Do you know, how a phishing attacker acquires your email address?

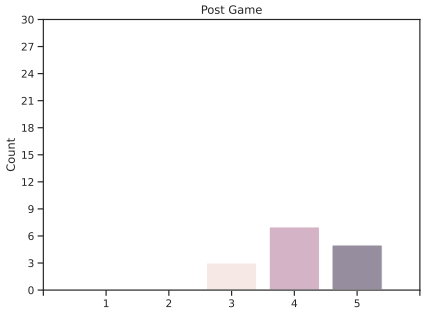

Figure 5: Answers to the question: Do you think the game "The get in" helped you to develop a better understanding about cyber attacks and cyberrisks?

engineering, the most common entry points for cyber criminals, current prevention measures taken actually make employees less robust against these attacks [8]. In order to increase awareness and understanding of common cyber threats we proposed a serious game instead of awareness campaigns. In this game the player takes the role of the attacker and gets insights on how attackers approach their targets and exploit common pitfalls. Attack based games are very popular in the cybersecurity world and are mostly encountered in the form of CTFs. These gameified scenarios, that usually correspond to real scenarios, have a huge learning effect but often require a deep technical understanding which makes them less accessible for a wider audience. Our approach is an interactive process in which the player is guided through different attack scenarios to make it more accessible. In each step of the attack the reasoning as well as options for prevention are is explained.

Based on our evaluation in section 5 we conclude that our game has a positive short term effect on increasing cybersecurity awareness. Furthermore, almost all participants that played the game stated that they enjoyed doing so. In order to mitigate the issue of the inequality of pre- and post game responses we could add a randomized session identifier to the pregame form that the player then should use for the game and the post form. With these measures we could filter out partial results and draw better conclusions. It is important to notice that we did not conduct a phishing awareness campaign before and after the participants played our game to verify the educational effects of the game in practice. The questionnaire itself also focuses more on short term results. As pinpointed in [21] there is currently no long term evaluation on the effect of serious games in a cyber security setting. We also leave that open as future work.

The game itself is currently in a development state and needs further refinement. Further it is questionable if the 3D setting adds any particular benefits other than mimicking AAA games. Especially for people that are not used to playing 3D games the more complex movement controls can potentially distract from the actual objective to highlight cyber risks. As the main focus of the game lies on scenarios which play on a computer (i.e. a 2D setting), the 3D graphics add more complexity than benefit for gameplay. The time spent on the added complexity of developing 3D games would be better invested in creating more sophisticated 2D scenarios, adding different difficulty options for each scenario or better image quality.

References

[1] Nmap. https://nmap.org/ Accessed on March 23, 2023.

[2] Owasp top 10. https://owasp.org/Top10/Accessed on March 23, 2023.

[3] Alabdan. Phishing attacks survey: Types,vectors and technical approaches. *Future internet*, 2020.

[4] Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf, and Imtiaz Khan. Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3:563060, 2021.

[5] Melissa Carlton, Yair Levy, and Michelle Ramim. Mitigating cyber attacks through the measurement of non-it professionals' cybersecurity skills. *Information & Computer Security*, 27(1):101–121, 2019.

[6] W Halfond, J Viegas, A Orso, et al. A classification of sql-injection attacks and countermeasures. In *Proc. of the IEEE int. symposium on secure software engineering*. IEEE, 2006.

[7] D Kennedy, J O'gorman, D Kearns, and M Aharoni. *Metasploit: the penetration tester's guide*. No Starch Press, 2011.

[8] Daniele Lain, Kari Kostiainen, and Srdjan Čapkun. Phishing in organizations: Findings from a large-scale and long-term study. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 842–859. IEEE, 2022.

[9] Marcel Maurer. Attack-simulation serious game for non-cybersecurity professionals. Technical Report 1, FHNW Master Thesis, fhnw.ch, 12 2022. Master Thesis at FHNW. Design and Development of the Serious Game to educate Cybersecurity.

[10] Nurul Amirah Abdul Rahman, I Sairi, NAM Zizi, and Fariza Khalid. The importance of cybersecurity education in school. *Int. Journal of Information and Education Technology*, 2020.

[11] Rohan Scanavez. Bad usb: why must we discuss this threat in companies? *Research Review*, 2(3):561–567, 2021.

[12] Christopher Scherb, Pascal Bürklin, and Christian Tschudin. Scoiot: Swarm-computations for the internet of things. In *2021 International Conference on Computer Communications and Networks (ICCCN)*, pages 1–6. IEEE, 2021.

[13] Christopher Scherb, Dennis Grewe, Marco Wagner, and Christian Tschudin. Resolution strategies for networking the iot at the edge via named functions. In *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2018.

[14] Bruce Schneier. *A Hacker's Mind*. W. W. Norton, 2023.

[15] Kurt Squire. Video games in education. *Int. Journal of Intelligent Simulations and Gaming*, 2003.

[16] Kevin M Stine, Kim Quill, and Gregory A Witte. Framework for improving critical infrastructure cybersecurity. 2014.

[17] Valdemar Švábenskỳ, Jan Vykopal, and Pavel Čeleda. What are cybersecurity education papers about? a systematic literature review of sigcse and iticse conferences. In *Proceedings of the 51st ACM technical symposium on computer science education*, pages 2–8, 2020.

[18] Michael F. Thompson and Cynthia E. Irvine. Active learning with the cyberciege video game. In *CSET*, 2011.

[19] Michael F. Thompson and Cynthia E. Irvine. Cyberciege scenario design and implementation. *Genetics Selection Evolution*, 2014.

[20] Michael F. Thompson and Cynthia E. Irvine. Cyberciege : A video game for constructive cyber security education. 2016.

[21] Jin-Ning Tioh, Mani Mina, and Douglas W. Jacobson. Cyber security training a survey of serious games in cyber security. In *2017 IEEE Frontiers in Education Conference (FIE)*, pages 1–5, 2017.

[22] Stella Vouteva, Ruud Verbij, and Jarno Roos. Feasibility and deployment of bad usb. *University of Amsterdam, System and Network Engineering Master Research Project*, 2015.

[23] Roselle L. Wissler, Robert B. Cialdini, and N J Schweitzer. The science of influence: Using six principles of persuasion to negotiate and mediate more effectively. 2002.