UNIVERSITY OF TARTU
Faculty of Science and Technology
Institute of Computer Science
Computer Science Curriculum

Santeri Rikhard Artturi Pohjaranta

Developing a Human-Centric Training Method to Educate High School Students on Social Engineering Techniques

Master's Thesis (21 ECTS)

Supervisor: Mubashar Iqbal, PhD

Tartu 2025

Developing a Human-Centric Training Method to Educate High School Students on Social Engineering Techniques

Abstract: Data security plays a vital role in our society. We use different tools for communication, such as social networks, emails, and phone messages. In the security of personal data, an important role play is technology, which collects and secures user data and the human who owns it. If technology helps to secure data, then the human role in the system is to hold access to their data and not give it to another person. From different papers, it could be found that the "*user is the weakest link in the security chain*". This happens because of various psychological manipulations that attackers use to receive sensitive data from users or, in other words, Social Engineering. To prevent such situations, people must be taught how attackers could receive their data through such manipulations and how to not fall into an attacker's trap by creating human-centric cybersecurity training. The current solutions lack a human-centered approach and platform tailored to high school students. Therefore, this research provides information about weak social engineering spots among high school students. Using knowledge about high school students' weak social engineering skills, this research presents a game-based training program using a one-platform solution to train high school students against current social engineering techniques with which they have problems. The efficiency of the training and platform is evaluated by the results of the first and second questionnaires to provide results of changes in the social engineering knowledge and skills of high school students.

Keywords: Social engineering techniques, Social engineering education and awareness, Cybersecurity education, Cybersecurity training, Human-centric cybersecurity training method, High-school students cybersecurity training

CERCS: P170 Computer science, numerical analysis, systems, control

Inimkeskse koolitusmeetodi väljatöötamine gümnaasiumiõpilaste harimiseks sotsiaalse manipuleerimise tehnikate kohta

Lühikokkuvõte: Andmeturbel on mängib meie ühiskonnas väga oluline rolli. Me kasutame suhtlemiseks erinevaid vahendeid, nagu sotsiaalvõrgustikud, e-kirjad ja telefonisõnumid. Isikuandmete turvalisuses mängib olulist rolli tehnoloogia, mis kogub ja kaitseb kasutajate andmeid, ning inimene, kellele need andmed kuuluvad. Kui tehnoloogia aitab kaitsta andmeid, siis inimese ülesanne süsteemis on hoida juurdepääs oma andmetele ega anda seda teisele isikule. Erinevatest artiklitest võib leida, et *"kasutaja on turvaahela nõrgim lüli"*. See juhtub erinevate psühholoogiliste manipulatsioonide tõttu, mida ründajad kasutavad tundliku teabe saamiseks kasutajatelt ehk sotsiaalse manipuleerimise kaudu. Selliste olukordade ennetamiseks tuleb inimesi õpetada, kuidas ründajad võivad nende andmeid saada selliste manipulatsioonide kaudu ja kuidas mitte sattuda ründaja lõksu, luues inimesekeskset küberturvalisuse koolitust. Praegused lahendused ei keskendu piisavalt inimeste vajadustele ega paku keskkonda, mis oleks kohandatud gümnaasiumiõpilastele. Seetõttu see uuring annab teavet gümnaasiumiõpilaste nõrkade sotsiaalse manipuleerimise kohtade kohta. Kasutades teadmisi gümnaasiumiõpilaste nõrkadest sotsiaalse manipuleerimise oskustest, see uuring esitab mängupõhise koolitusprogrammi, mis kasutab ühtset platvormilahendust gümnaasiumiõpilaste koolitamiseks tänapäevaste sotsiaalse manipuleerimise tehnikate vastu, millega gümnaasiumiõpilastel on probleeme. Koolituse ja platvormi tõhusust hinnatakse esimese ja teise küsimustiku tulemuste abil, et näidata gümnaasiumiõpilaste sotsiaalse manipuleerimise teadmiste ja oskuste muutusi.

Võtmesõnad: Social engineering techniques, Social engineering education and awareness, Cybersecurity education, Cybersecurity training, Human-centric cybersecurity training method, High-school students cybersecurity training

CERCS: P170 Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine

Acknowledgements

Supervisor

I'd like to thank my supervisor, Dr. Mubashar Iqbal, for helping me by providing guidance in writing my thesis and connecting with people who helped me with questionnaires and consent forms. He always answered my questions, even if it included knowledge that I was required to have.

Consultants

I'd like to thank MSc Terje Mäesalu for validating and providing ideas on improving the consent form.

I'd also like to thank MSc Mari Seeba for validating and providing ideas for the first questionnaire.

Use of AI

Grammarly

Grammarly[1] is an AI-powered tool for text correction that clears mistakes and suggests improvements for in-text writing. Grammarly AI-powered software is a great tool for correcting mistakes in text and raising grammar levels. His AI algorithm helps adjust sentences so that they show better by the provided parameters. Also, his new feature to check text on plagiarism helps to find sentences that are not written by the author intentionally or unintentionally and change them.

ChatGPT

In the process of writing this thesis, I used ChatGPT V3.5. ChatGPT[2] is a bot that uses an advanced AI language model to understand human commands and provide results as if a person using ChatGPT were talking with another human. His deep language model offers efficient results with low time response. He was helpful in generating questions for the second questionnaire and translating the text for a game in Russian and Estonian.

[1] https://www.grammarly.com
[2] https://chatgpt.com

Contents

1 Introduction **7**
- 1.1 Problem statement . . . 8
- 1.2 Research questions . . . 8
- 1.3 Research method . . . 9
- 1.4 Contributions . . . 10
- 1.5 Thesis structure . . . 11

2 Background **12**
- 2.1 Social engineering . . . 12
- 2.2 Human-centered aspects . . . 24
  - 2.2.1 Approach . . . 25
  - 2.2.2 Design . . . 25
- 2.3 Training techniques . . . 28
- 2.4 Gamification . . . 30
  - 2.4.1 Types of games . . . 30
  - 2.4.2 Game genres . . . 30
  - 2.4.3 Game mechanics . . . 31
  - 2.4.4 Gamification frameworks . . . 32
- 2.5 Summary . . . 34

3 Research Protocol **35**
- 3.1 Selection of social engineering techniques . . . 35
- 3.2 Design and implementation of two-phase testing protocol . . . 37
- 3.3 Phase-I questionnaire . . . 38
- 3.4 Phase-II questionnaire . . . 38
- 3.5 Consent form . . . 38
- 3.6 Pilot study . . . 39
- 3.7 Summary . . . 39

4 Results of Phase-I Questionnaire **40**
- 4.1 Demographics . . . 40
- 4.2 Knowledge of social engineering techniques . . . 43
- 4.3 Skills against social engineering techniques . . . 44
- 4.4 Key takeaways . . . 63
- 4.5 Summary . . . 65

5 Gamification-based Training **66**
- 5.1 Training program . . . 66
- 5.2 Game creation . . . 67

5.2.1 Game description 67
5.2.2 Analysis of game through framework 69
5.2.3 Game development tools 71
5.2.4 Game scenarios 75
5.2.5 Game mock-up 77
5.2.6 Game code examples 78
5.2.7 Game testing 81
5.2.8 Game prototype 85
5.3 Summary 92

6 Results of Phase-II Questionnaire **93**
6.1 Second questionnaire 93
6.2 Results of second testing 93
6.3 Summary 107

7 Conclusion **108**
7.1 Answer to research questions 108
7.2 Limitations 109
7.3 Future works 109

References **113**
II. Licence 114

1 Introduction

People use different technological tools for work and in their daily routines: communication, banking, entertainment, etc. By using such devices in some of them, people provide personal information, which is needed to identify humans who use such tools. Organizations use different technological solutions to store this data safely. But, if human data is stored somewhere on the server, then there needs to be a human to whom this data belongs. If we compare humans with written code, humans are more complicated objects with different behavior and psychology, and based on that, they could act on things differently. Because of that, for example, if the first person finds the right path to talk with the second person, then the first person could easily manipulate the second one and receive safely stored data. Because of that, it is essential to teach people how to react to specific situations so that their personal data does not pass into the wrong hands.

First, we must understand that situations where attackers use behavior or psychological methodology in cyberattacks are called social engineering [16, 11, 3]. It is a type of cyberattack where the attacker uses psychological manipulations to reach the target and make him do what the attacker says. The types of attacks could differ according to what the attacker would like to receive from the target and who the target is. Papers about social engineering indicate different results on different attacks, but they have one common point: many people need to learn about Social Engineering and attacks that could be used against them [5, 1, 3, 7, 46, 39].

In 2022 was done a research that provide example of how people react differently to Social Engineering threats. The main focus of the research was to measure human vulnerabilities in the area of social engineering, phishing, and password attacks, provide analysis details, offer suitable solutions to close the gap in knowledge of social engineering [5]. The data provided by the questionnaire were separated by age, sex and job type. In this research interesting for us is to see difference in age and sex. By the end of the research, there was no significant difference between men and women in such fields, but still a little difference in password sharing and anti-spam program use. By age was found that older people have more problems with social engineering than younger people. Another research was provided in 2021 that checked the knowledge of different age groups in social engineering [7]. The results show that people know less about Social Engineering and how it works with age rising. This also indicates that young people know much more about Social Engineering. The interesting was that such papers on Social Engineering knowledge related to people who are above 18 years. Most research papers provide results on knowledge and skills in social engineering starting at 18 years of age, and in most cases these people already work or study at university. Because of that, we do not have a clear picture of how well this thesis about understanding social engineering threats with age rising correlates with high school students' knowledge and skill in this area.

From this point, we have a question: *Do high school students have knowledge and*

skills against Social Engineering threats? If not, in which area do they have weaknesses, and how do they prepare for dangerous situations in the future related to current known social engineering threats?

1.1 Problem statement

Social engineering involves many techniques (as discussed in Section 2.1) that can be used to manipulate someone. The attackers try new ways to manipulate other people with their tools, there will always be a cycle of creating a new technique that needs to be investigated and found countermeasures. Because of that, it is essential to provide proper education about social engineering and constantly update it based on new findings and techniques [5, 1, 3, 7, 46, 39].

The current solutions lack a human-centered approach tailored to high school students, and also, such platforms fail to aggregate social engineering techniques into a single platform. So the knowledge about social engineering techniques and how to mitigate them is scattered on many different platforms [31, 42, 34]. Furthermore, the existing solutions do not provide a dynamic way to add new social engineering techniques once they appear. For example, Deepfake or QRishing social engineering techniques have emerged recently. Still, few people understand how to mitigate them because the existing social engineering education resources are not updated or do not have the proper functionality for providing information about such techniques [45, 35].

1.2 Research questions

To address the aforementioned research problem, we have devised our main research question to educate high school students about emerging social engineering techniques. The main research question is future divided into two sub-research questions (SRQ).

[RQ]: How to educate school students about social engineering techniques?

[SRQ1]: In which social engineering techniques do high school students require education?

SRQ1 is related to exploring high school student knowledge about social engineering techniques and how well they mitigate them. There are not many studies conducted to explore how much high school students know about social engineering and techniques and also how effectively they mitigate specific social engineering techniques and which exactly. This research explains how well high school students mitigate social engineering techniques from their age and gender perspectives.

[SRQ2]: How to build a practical training platform to educate high school students about social engineering techniques?

As part of this research, we create training program to close gaps in vulnerable areas of social engineering attacks. Tasks in created training based on situations from the real world to imitate situations in which the target group could find themselves and help to receive an experience that could be needed in the future.

1.3 Research method

The start of the research process would be reviewing different social engineering techniques and choosing suitable for a questionnaire that tests how high school students mitigate social engineering techniques and their knowledge in this area. After analyzing the results, specific social engineering techniques for which high school students are more vulnerable will be chosen. These techniques would be used in a new training program, which would be tested on the same group who passed the questionnaire with using a one-platform solution. This is required to understand if provided training closes gaps in knowledge of social engineering techniques found earlier.

In the process of receiving results, we review information that helps create a training program. It includes different training techniques to understand which training format is suitable for our training program and related to this technique elements.

When results are reviewed and all elements required for training creation are found, this information will be used in training creation. The training program has such steps:

- Prototyping idea for training and related with it elements
- Writing a scenario that training provides content in an understandable format for the target audience
- Testing to understand if all steps of the training program work as planned

After all the tests, the same people who had passed the questionnaire would go through the training program. To understand how well this training program helps them close their gaps in vulnerable areas of social engineering, they will pass a second questionnaire. The second questionnaire has questions related to attacks used in the training program. After receiving results, answers from the first and second questionnaires would be compared to see how their skill in mitigating social engineering attacks is changed.

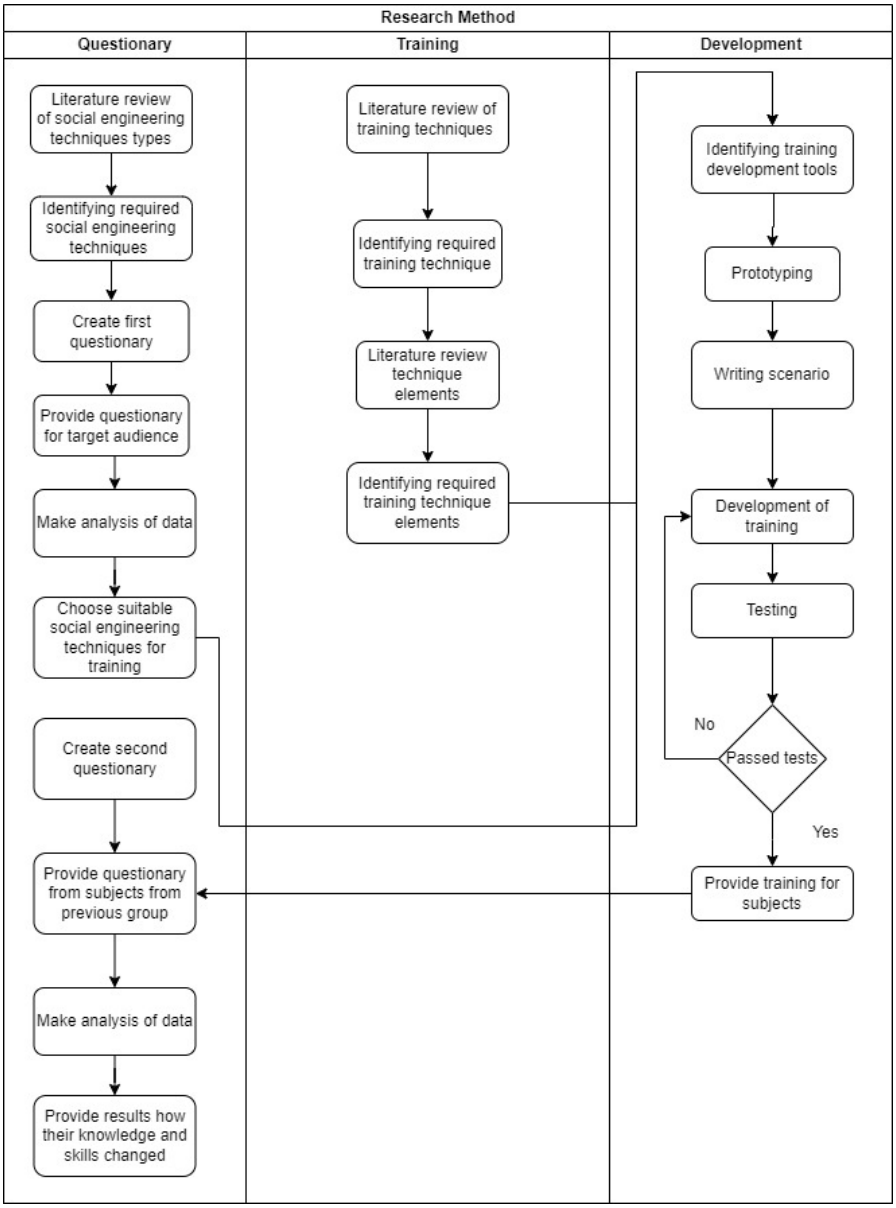

Figure 1. Research method

1.4 Contributions

The main goal of this thesis is to provide a one-platform training solution for comfortable education and opportunity to add new tasks related to social engineering attacks. For that, we need to analyze the current knowledge of the subject for who we do this solution and how to prepare material that they understand and use it. Three main contributions

are made. The contributions are as follows:

- **[SRQ1]** aims to highlight high school students social engineering attacks knowledge on the current moment in Section 4
- Analysis of current solutions and methods which are used for training social engineering attacks answer on question **[SRQ2]** only on half in Section 2.
- Another half answer on **[SRQ2]** from the practical side in Section 5 as a proof of concept of a one-platform solution and show the results of it in Section 6.

1.5 Thesis structure

This thesis is split into different sections. It has information on research papers that was done earlier to describe existing gaps in the field of social engineering in cybersecurity; information on different methodologies to understand ideas which are used in research and why it is important; creation process of the training program; conclusion with results of training and ideas on what could be done in the future.

2 Background

This section provides basic information that is required for research work. It includes information related to human psychology inside and outside cybersecurity, social engineering, gamification techniques, training models, and prototypes that were used and tested. Also, this material helps to answer SRQ2 from Section 1.2 as a base for the created training platform.

2.1 Social engineering

Let us start with the main topic of research, social engineering. It is a complex topic that have different meanings based on the situation in which it is used. From the original meaning, social engineering is a manipulation of human beings to create a mindset in their minds that they can trust [19]. In the computer science, social engineering is described as a set of methods used to manipulate people to receive critical information from the target or manipulate the target for action that could be profitable for the attacker [38, 42, 1].

Humans can be manipulated differently based on the approach that attackers use. By classification, social engineering attacks could be separated into a human-based approach when the attacker executes the attack by himself and a computer-based approach when the attacker uses software to automate actions related to the attack [38, 11].

In the human-based approach, attacker contact with the target could happen directly or indirectly. For example, direct contact is when an attacker talks with the target and influences the target using human psychology and soft skills. In an indirect situation, an attacker creates a social media account and starts chatting with target using the same methods as in the direct approach [11]. The main difference between the direct and indirect approach is that when an attacker talks with target from the internet, he has less chance to be identified and more time for better answers. Using a human-based approach, an attacker could use different methods of human manipulation based on the target profile, but the number of people on which it could be used is less because the attacker must prepare for each target, which takes a lot of time.

Computer-based approach use tools that create content for target manipulation. This approach uses indirect communication methods with the target, including automatic e-mail sending, bots for social media sending, and other tools that help automate attacker work. By using such an approach, the target amount is more considerable. Still, because the content is created based on the profile of a specific group of people, it could only work sometimes as expected because the attacker needs to know the actual profile of the person who receives such content.

Cybersecurity social engineering has different techniques based on how the attackers try to receive data from the target based on the amount of targets and required information. Below is a list of methods that are known:

Technique	Method	Detail
Phishing	Any communication tool	Attacker obtain target information by sending message using any existing communication tool.
Vishing	Phone calls	Attacker psychologically manipulate target using a phone for communication.
Smishing	SMS message	Attacker send to target SMS message which could have a malicious link to a website or provide instruction what target needs to do.
Whaling	Malicious emails	Attacker send an email message to organization high-level executive with malicious link or message with instructions.
Spear Phishing	Collection of data about target	Attacker collects information about the target and, use it for psychological manipulation.
Pharming	Create a clone of original website	Attacker clone original website and use it to collect data from target(-s) who think that this website is legitimate.
Angler phishing	Impersonating as a worker of organization	Attacker impersonates himself as a legit organization worker and creates an illusion that he deals with customer problems, in this time, he asks target to provide required for attacker information.
Grooming	Psychological manipulation	Attacker try to get into contact with children and by psychological manipulation try to receive intimate information.
Pretexting	Collect target activity information	Attacker collect target activity information and by that tries to receive the target personal information by providing work application or any activity which requires personal information.
Profile cloning	Clone of the legit organization profile	Attacker clone legit profile of the legit organization and use it to collect information from customers of this organization.
Face-to-face interaction	Interaction between two persons in real life	Attacker starts a conversation with the target in real life and by psychological manipulation receive information from target.
Shoulder surfing	See from shoulder	Attacker stay behind the target and from the shoulder of target see all that target do.
Quid pro quo	Provide service for target	Target gets in contact with the attacker and asks to do service with his device, which the target cannot do himself. When the attacker receives a device from the target, he also receives the target's credentials and personal information.
Dumpster diving	Information search	Attacker receives information from a source which is no longer in use but could be valuable for future use.
Diversion theft	Physical contact with the device of attack	Attacker use service organization who do maintenance of other organization IT infrastructure and with their help install malware in target organization infrastructure.
File masquerade	Hide malicious file on target workstation	Attacker set on target workstation malicious file which is named or has an icon of the legit program or file on target workstation.
Reverse social engineering	Make problem for the target and help him	Attacker make problem for the target and the target asks the attacker to solve a problem which target could not solve with his own skills.
Scareware or *Pop-up window*	Pop-up message with a link to malicious code	Target receives a Pop-up message on a webpage that his workstation is infected by malware. When the target clicks on the provided link by attacker to clean his workstation, it downloads on the target workstation malicious code.
Water-Holing	Code payload injection	The attacker sends a payload of malicious code on a website that the target used recently and waits until the target does some action to activate the payload that infects the target workstation.
Tailgating	Impersonating as someone else	Attacker tries to receive access to places he does not have access. It is done by personalizing himself as someone who have access.
"Evil Twin" WIFI or WiPhishing	Legit WIFI clone	When target try to connect to WIFI hotspot he could connect to a copy of a legit WIFI hotspot, which gives access to his traffic to attacker.
QRishing	QRcode	When a target scans QRCode, it redirects it to a malicious website.
Deep fakes	Fake images creation software	Attacker create a fake image or video and use it for manipulation of the target person or group.

Table 1. Social engineering techniques

Phishing techniques receive targets data by sending trustful messages by any communication tool with instructions [38, 11]. It could be used with malware, bots, and trojans to obtain access to targets data and could be combined with other types of attacks. For example, this method of attack uses emails with malicious links or files. It can also use a website that is a clone of an official organization that a target trusts [4]. In 2020, a study checked how well school children aged 12-14 and 15-17 can detect phishing emails. Overall results for 12-14 age old was 59 percent and for 15-17 was 59.5 percent [32].

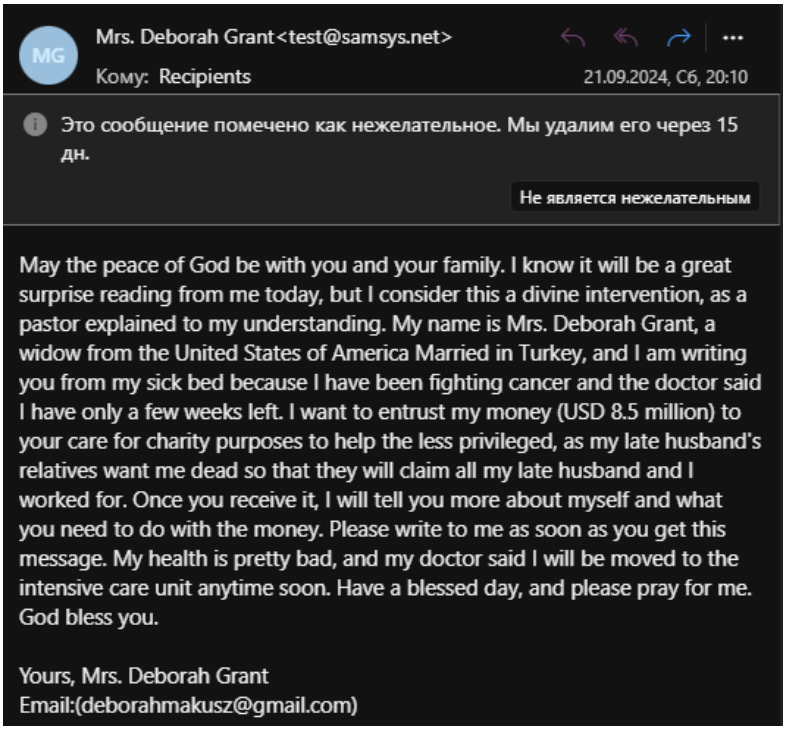

Figure 2. Phishing example

Vishing is phishing attack that uses voice communication as the primary tool against the target [38, 11, 4]. For example, the attacker impersonates as someone from the official organization, like a bank worker or police officer, and by describing a situation that something is happening with the target property or a case related to the target, tries to receive sensitive information. In 2020, an incident happened when an attacker using an AI voice made phone calls to Ritz London clients and convinced them to give the attacker credit card information [16].

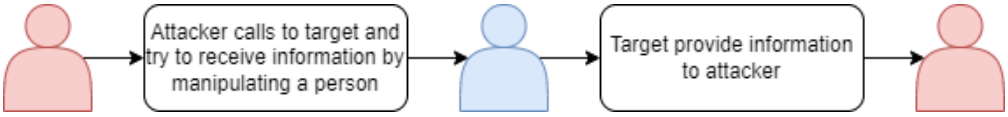

Figure 3. Vishing example

Smishing is a phishing attack in which the attacker sends SMS messages to the target. SMS could contain links to malicious websites or text that require the target to send personal information to the same number in SMS format [28]. In 2023, a study showed injection success, which was tested on different demographic groups. In this study injection rate in high scholars group was 20.00 percentage [37].

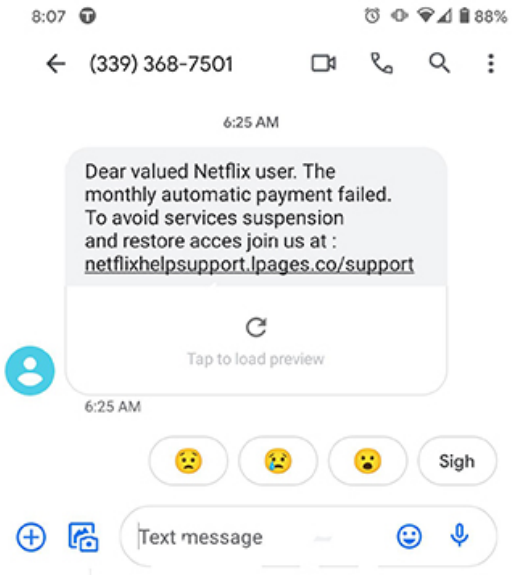

Figure 4. Smishing example, adopted from [14].

Whaling is a phishing attack targeted at the senior executive in organizations. An attacker masquerade phishing message as a legitimate and send it to target organization. If the attack is successful, the attacker receives critical information about the organization, such as credentials of people from the organization or access to organization infrastructure [28]. As an example of such an attack, an attacker sends an email with a malicious link. The link contains the organization's cloned application, which a person uses for authorization. When a person sends his information to the application, the attacker receives it and can gain access to the organization's servers.

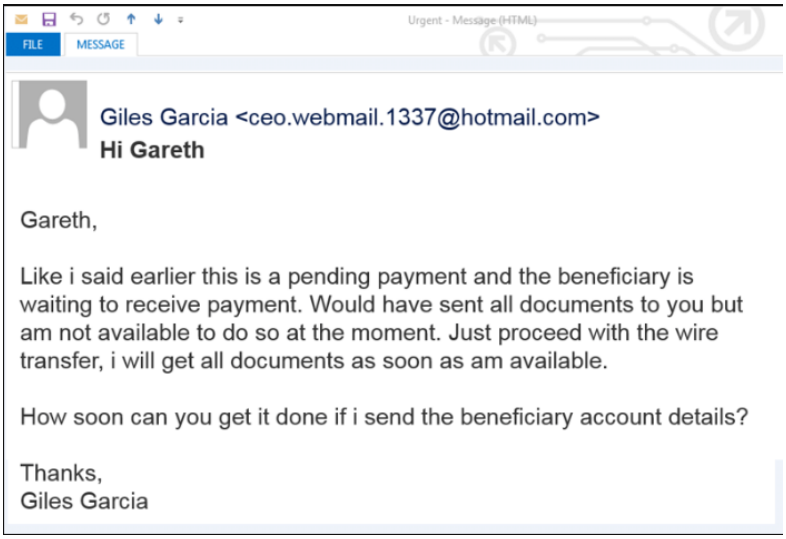

Figure 5. Whaling example, adopted from [41].

Grooming is a type of cyberattack where the target is children. An intruder goes into trust with a child to obtain intimate and personal data (often sexual such as sexual conversations, pictures, or videos) to threaten and blackmail for further inappropriate material [38].

Shoulder surfing is when someone is behind the target and sees the target data on the workstation [29, 39, 11].

Dumpster diving attack is attacker receives information that is no longer in use and could be valuable for accessing critical data [38, 39, 11].

Spear Phishing is phishing attack in which the target is a person or group on which the attacker has collected data [38, 21]. Before an attacker starts his attack, he collects data about the target to understand his psychological profile. With this knowledge, the attacker would have more influence on the target, which raise success of injection.

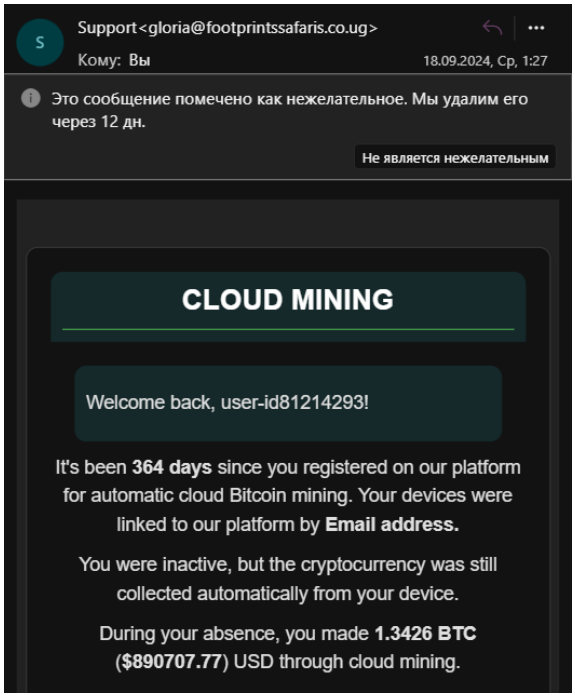

Figure 6. Spear Phishing example

Pharming is an attack in which the attacker creates a copy of the original website or profile and uses it to collect data from the target, impersonating itself as legitimate. For example, first, the attacker installs malicious software on the target computer, redirecting him to the prepared website. Second, the target opens the prepared website, and the attacker receives data from user input [29, 38, 26].

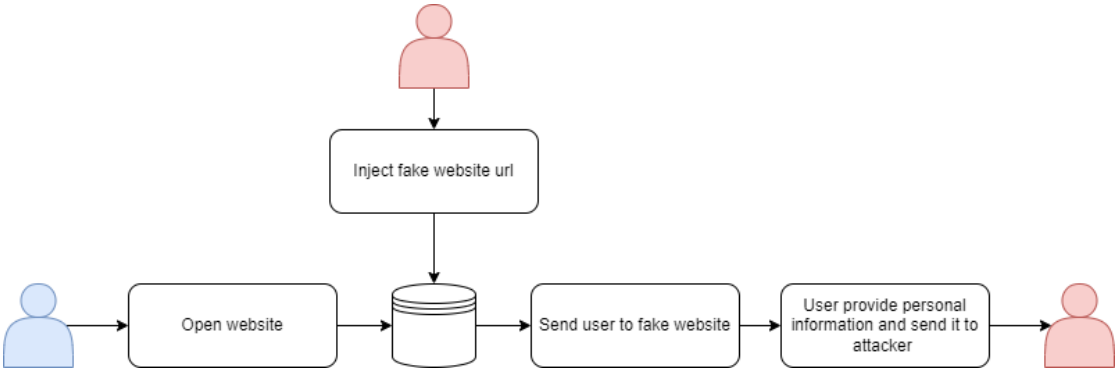

Figure 7. Pharming example

Angler phishing is an attack type where the attacker impersonates himself as a contact person who deals with customer problems and, by communicating with the customer, receives data from the customer. For example, customers write bad reviews on products on Amazon or Aliexpress. The attacker creates an account on this service where he writes in his profile that he is dealing with customer problems. The attacker contact this customer and provide his help to deal with his problem. Still, instead, the attacker's actual goal is to collect personal information from the customer [29].

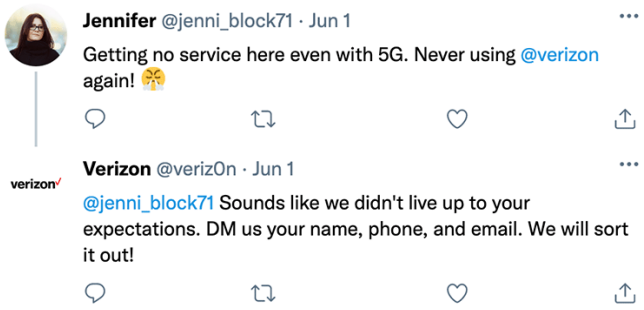

Figure 8. Angler phishing example, adopted from [25].

Pretexting attack starts with collecting user activity. The attacker uses this information to receive personal information from the target by providing a job or offer for an activity close to the target's previous activity [38, 39].

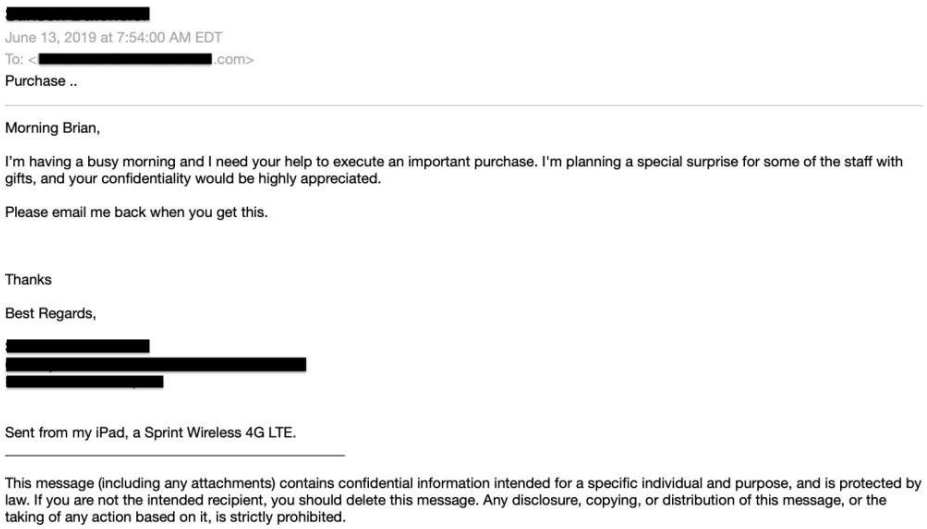

Figure 9. Pretexting example, adopted from [17].

In *Profile cloning*, the attacker clones the profile of the user or organization and uses it to collect information from the target, impersonating himself as a user that the target can trust[38, 39].

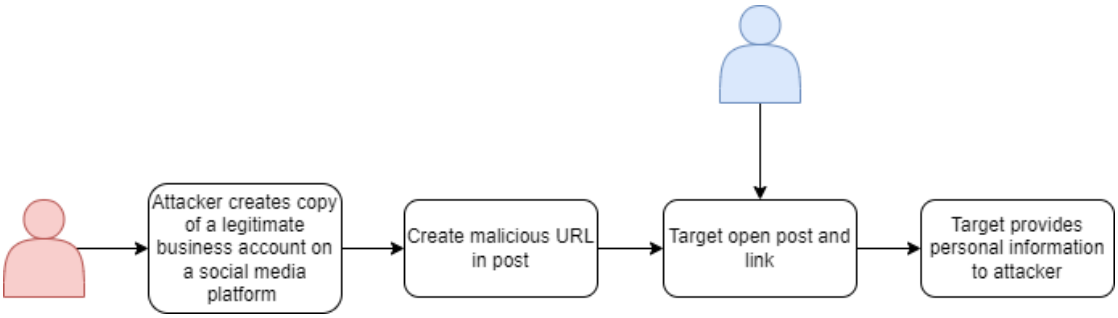

Figure 10. Profile cloning example

Face-to-face interaction is an attack in which the attacker interacts with the victim personally and uses psychological techniques to manipulate the person [39]. This attack requires good soft skills (skills in communication in real-time) and an understating of human psychology, such as fast changes of voice tone and body language and creating a psychological portrait of the target.

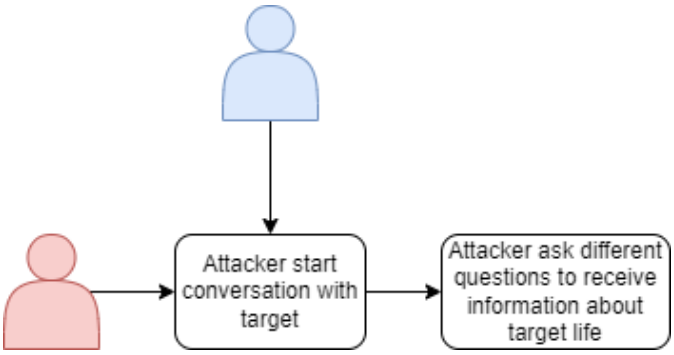

Figure 11. Face-to-face interaction example

Quid pro quo attack is an attack requiring the target to ask an attacker to help solve problem beyond target ability. For example, to remove virus from computer. The attacker receives the computer and credentials from the target [29, 39, 11].

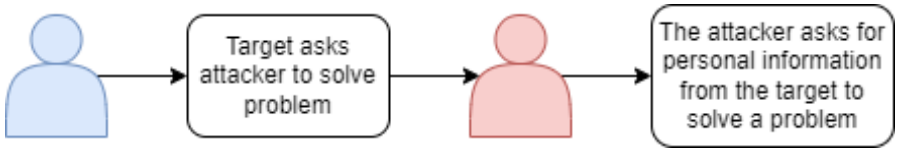

Figure 12. Quid pro quo example

Diversion theft attack use service companies that install, maintenance hardware or software. The attacker uses them to install malicious code with their service as legitimate software that no one notices [39, 38].

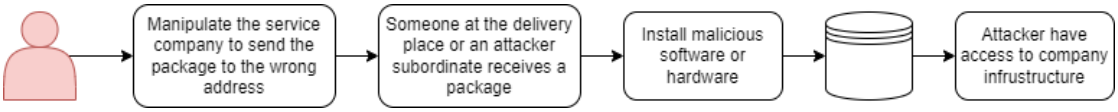

Figure 13. Diversion theft example

File masquerade hide malicious file stored in a bunch of other files on the target computer. This attack plays on the user's mind that all files on his computer are safe [39].

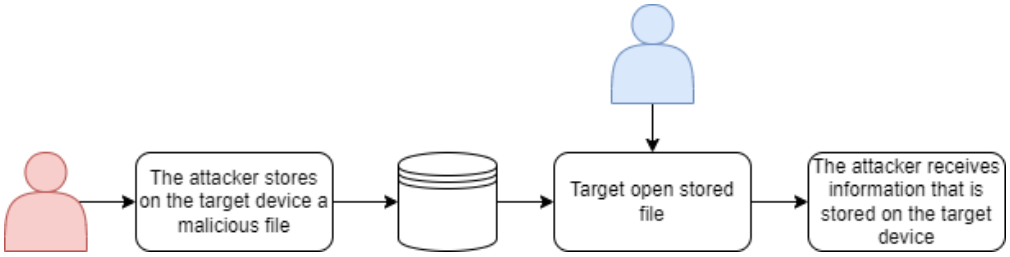

Figure 14. File Masquerade example

Reverse social engineering attack is same as "Quid pro quo attack" but the intruder makes problem for the target first. The attacker creates issues, for example, with target internet network, then manipulates target so that attacker provides high-quality service that will solve target problem and, by that receive access to target data [39, 38, 29].

Scareware or Pop-up window is an attack that shows a Pop-up message for the target on the website, and by clicking on that, the target installs malicious code on his computer. For example, when the target goes on the webpage, he receives a Pop-up message that his computer is infected with a virus, and he needs to download software using the provided link. When the target clicks on that, he downloads a virus on his computer or gives the attacker access [39, 39].

Figure 15. Scareware example, adopted from [44].

Water-Holing attack load malware on web resources using high traffic as eyes through. Wait until the user clicks on a specific item to activate malware [39].

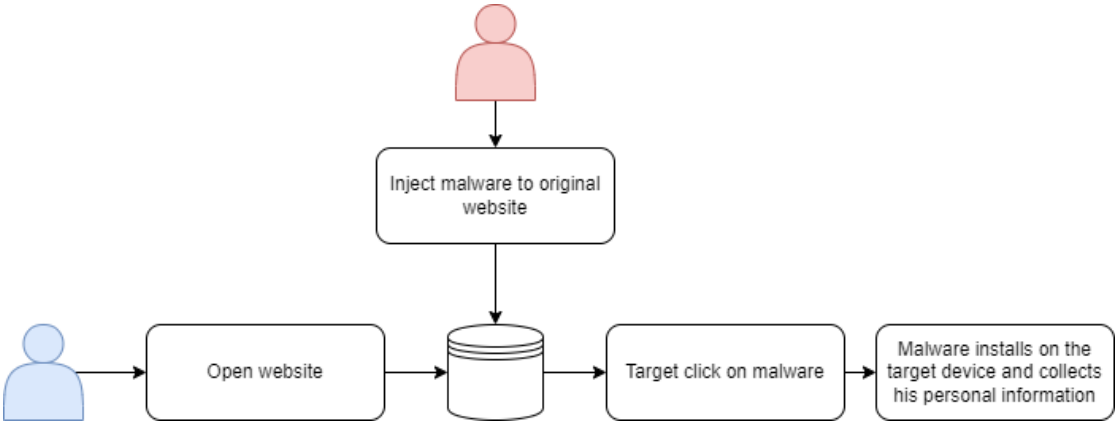

Figure 16. Water-Holing example

Tailgating work if attacker receive access to a restricted area by pretending to be a personal who has access to it but does not have key to place with him right now [39, 38, 11].

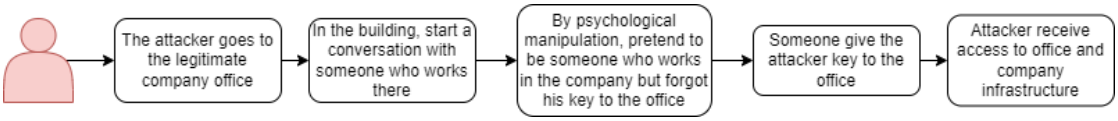

Figure 17. Tailgating example

"Evil Twin" WIFI or WiPhishing create a copy of a legit WIFI hotspot that gives intruder access to your computer from the "Evil Twin" network. For example, when the target tries to find a free hotspot in the airport. The attacker creates wireless network access by his laptop or device where the target could connect and give the name of a legitimate airport WIFI. When a target is near the attacker, the target sees that this hotspot connection is excellent and open for useage. Target connect to this WIFI and use WIFI. Meanwhile, attacker, by the application that could see the network activity of target, collects information about this person. An attacker receive target credentials if the target uses web services that are not secure from wiretapping [9, 41].

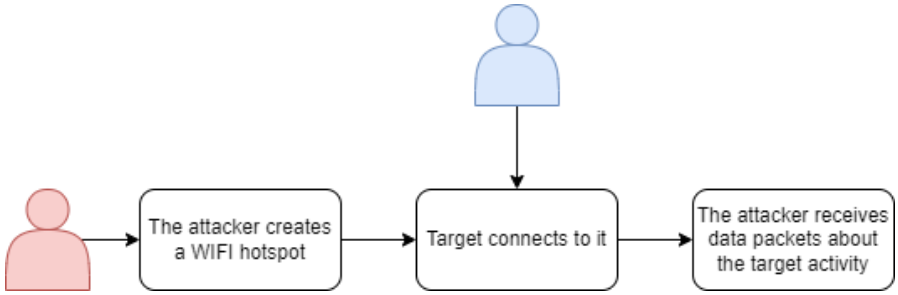

Figure 18. WiPhishing example

QRishing uses QR codes to lead the target to a link with malicious code. For example, when someone puts his own QR code to an event poster as legitimate, an attacker sees it. He changes the QR code on the poster to his. When someone scans it, the QR code sends a person to a malicious web service [43].

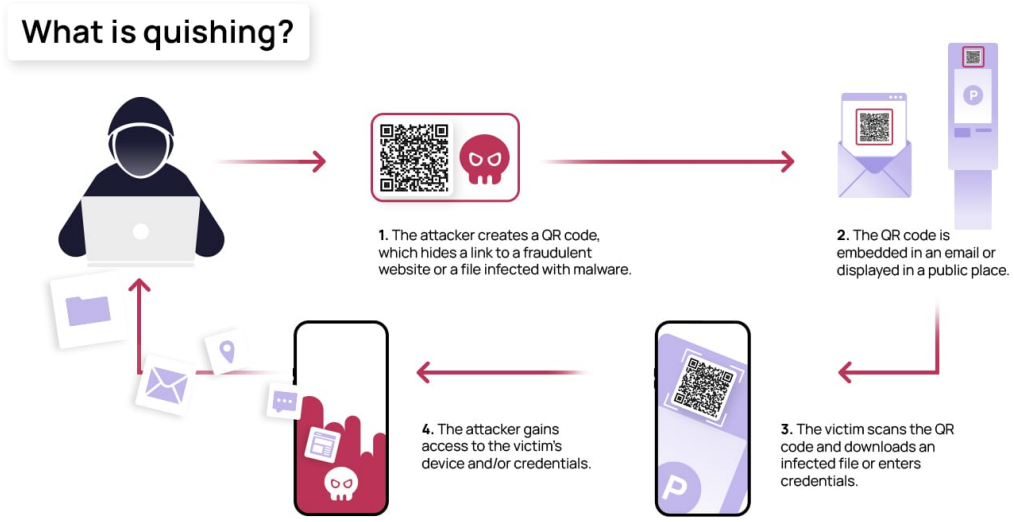

Figure 19. QRishing example, adopted from [40].

Deep fakes is a digital content created by deep learning tools, primarily used in media. For example, when a person takes a photo of a popular person and, by using AI, creates a video based on an event and places the face of this person in this video [35].

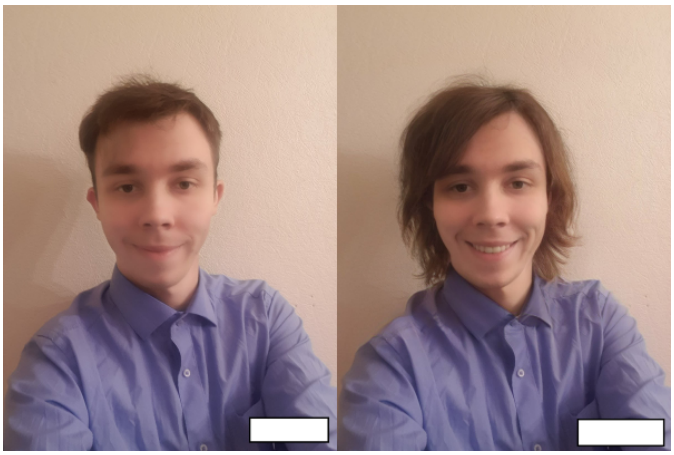

Figure 20. Deep fakes example

As you can see, social engineering has many different techniques, and the specter of how attackers use them could be different. But some of them could be combined to create a more complex attack. An example of such an attack was when attacker created a McDonald's account on Facebook and posted coupons for lower prices of meals [10]. When a target sees these coupons, he tries to receive them but was required to send information about credit card. As you can see here could be found Profile cloning of a McDonald's account and impersonating it as a legitimate account of the brand on Facebook and a Phishing person who like to receive free coupons but lost his data to the attacker. Also, if coupons were not used in other McDonald's products, they are deep fake images of coupons.

2.2 Human-centered aspects

Section 2 described the main topic of this research, and if described briefly, social engineering deals with manipulating the human mind. From a security perspective, technical countermeasures only temporarily affect user security because attackers always try to find a new approach to their target in social engineering. So, if train someone, training needs to include the human factor as part of the security system so that the user can adapt to the situation by using learned information, and the system could adapt to user current needs, future needs, and additional training. Human-centered aspects help to understand the parts needed to include users in such a construction.

2.2.1 Approach

Let's start with understanding what is in a human-centered approach. The main idea behind it is that the system needs to change to the user's current needs, adapt to be relevant with standards and principles in design, and be user-friendly for better-involving users into the system [27].

"Systems feature simplicity in understanding and operation, thereby diminishing expenses related to training and support" [27]. Because the human-centric approach is built not around a specific group but provides a solution that is comfortable for all users who would like to try it, the system needs to be built as efficiently as possible so that users would not feel frustrated. Such a way helps also lower costs on other things related to development and maintenance.

"Decreased discomfort and stress lead to enhanced user satisfaction" [27]. When working on a task, users could start to feel discomfort based on the level of knowledge required to finish the specific task. This could lead to a drooping task before the user can finish it. Because of that, the product must be built so that the user who uses it feels satisfied with his understanding of using it or knowledge about specific elements.

"Users productivity and organizational operational efficiency witness improvement" [27]. Users use specific products to solve their problems. Suppose a product solves a particular problem for the user. In that case, it should provide specific improvements in user metrics such as productivity or efficiency.

"Enhanced product quality, aesthetics, and impact lead to the potential for gaining a competitive" [27]. The product needs to have an idea behind it and provide content that is in good shape so that user will like it and it solves their problem or provides them with something new.

2.2.2 Design

The main focus of design in human-centered aspects is that users feel comfortable and interested in working with the system and providing the information that users need. If describe how the system needs to be designed, need to remember that:

"Engaging users actively in the design process and gaining a clear understanding of their needs, tasks, and requirements" [27]. One way to provide the required elements in system design is by engaging users to help with the project. If the user likes the project, he could help with his skills, which could be required for specific project parts.

"Allocating functions appropriately between users and technology, delineating which tasks users can undertake" [27]. Users need to feel comfortable dealing with specific tasks in projects. But it does not mean that all functionality needs to be put on code. If automating the process by a maximum, the user would feel bored and less interested in the product, which works without actions from his side. Need to balance functionality from the projects backend and provide user activity.

"Iterating on design solutions, with user feedback serving as a pivotal information source" [27]. As was said earlier, the human-centric approach is built around users who use this specific product. This principle also goes into design that all elements must be built around users needs. However, all feedback from the user needs to be analyzed and integrated into the system, not directly incorporating user ideas into the system. Users could have proposals about the functionality of the product. Still, it needs to go from the developer on how to integrate it based on project documentation and analysis of user needs.

"Adopting a multidisciplinary design approach that necessitates diverse skill sets. Interdisciplinary design teams should comprise end users, buyers, business analysts, domain experts, systems analysts, programmers, and marketing and sales professionals" [27]. Not only users need to feel comfortable with the project, but also people who help build it. The development of a project is a vast mechanism, and if these parts start to work poorly, it will break the work process. It is essential to have a healthy environment around the project, which helps integrate new ideas and improves the productivity of the whole project.

"To better understand how to design a system, remember that good design means good usability to the user. What exactly does good usability mean? It means a system that provides all expected functionality that the user needs" [27]. For example, when someone solves a quest in the room, the organizer provides the user only the tools and information he requires to solve the puzzle. In this situation, he feels more comfortable than when he has visual details on something that is not used in a quest or when he has an additional tool that is not used. If describe usability criteria, then they are:

Effectiveness - see how users accomplish specific objectives, measured by accuracy and completeness with which users achieve specific objectives [27].

Efficiency - measures the relationship between the accuracy and completeness of users achieving specific objectives and the resources expended to achieve them [27].

User satisfaction - indicates the level of comfort and positive attitudes a user has towards utilizing the system [27].

Ease of learning - encompasses how effectively users interact with the system, including both functional and non-functional elements. Non-functional requirements may contribute to user comprehension of system elements or provided information [18].

Flexibility - the ability of a design to accommodate and adapt to the diverse needs, preferences, and skills of human users.

Ease of recall - user's ability to remember how to use a product, service, or interface without needing to relearn it each time they interact with it.

Ease of use - denotes how well the design prevents errors or aids in recovery from those that occur [27].

Error tolerance - That is how well the product supports initial orientation and deep understanding of its capabilities.

In the process of planning human-centred design needs to remember such things as: "Identifying appropriate methods and resources for the activities" [20, 27, 22]. Because the human-centric approach focuses on users having only essential resources, the system must have nothing to distract the user.

"Defining procedures for integrating these activities and their outputs with other system development activities" [20, 27, 22]. Later, when the system is in development, anything could happen during this process, and plans could change. Some features would be thrown out, and some stay in development status. Remember that features that are developed for the system are essential parts of it, so if some feature works incorrectly or disturbs another, it would create a bad experience for the user.

"Identifying the individuals and the organization(s) responsible for the human-centered design activities and the range of skills and viewpoints they provide" [20, 27, 22]. Because the system must go through the development cycle at the right time, finding people who could provide such a service is crucial. Also, it is essential to maintain their work while working with some part of the system and control if their work does not hurt the system.

"Developing effective procedures for establishing feedback and communication on human-centered design activities as they affect other design activities and “trade-offs”, and methods for documenting outputs from these activities" [20, 27, 22]. All good things start their process from the beginning. It is essential to receive feedback about system work from a user perspective and its effect on partners. Because new system development takes a lot amount of work, we need to understand how effectively partners work with different parts of it and how to help them.

"Agreeing on appropriate milestones for human-centered activities integrated into the overall design and development process" [20, 27, 22]. The system requires only the needed features to be completed and used by the user in the project design. Integrating features that will not be used in the system would be wasted time. Adding features that are made poorly or do not have proper functionality would irritate users.

"Agreeing on suitable timescales to allow iteration, use of feedback and possible design changes to be incorporated into the project schedule" [20, 27, 22]. Such projects are created by people with different specializations, such as marketing, branding, sales, technical support and maintenance, health and safety, user interface, visual and product design, user management, service management, and corporate governance. Because these people have different work, experience, and skills, they need to find a compromise on the amount of work and timescale that would positively affect their work and bring positive changes in system development and maintenance.

In planning the system, need to go through activities that help better understand the project's details built by a human-centric approach [22]. These activities are:

- understanding and specifying the context of use
- specifying the user requirements
- producing design solutions
- evaluating the design

Let's discuss each of these activities to understand better what is needed. First, let's start with **understanding and specifying the context of use** [22]. All projects have their problem solution, which they try to solve for the users. How well they do that depends on the tools used to work with the system. Using different metrics, developers can understand how many users need features in the project and create the proper context for the whole project. Because the system is built around the users, it is essential to have information about different aspects of the system's work, partners, and users. This information would help create the proper context for the system's work.

Next, when the project has information about different aspects of project work, it is essential to understand what "exactly" the users need. Providing the proper description term "exactly", it means features that create good usability for the users. This includes technical and non-technical requirements. As an example, one of the non-technical requirements is that the application has a specific catalog of colors used. For that, we need to identify active application users and their application requirements. Also, think about other parts of the system that do not directly work in the application but have a connection with it. For example, when someone has difficulties with an application, they call the call center to ask for help. In that situation, the requirement could be that the user's maximum wait time is 30 seconds [22].

When someone produces a design for an application using a human-centric approach, project requirements do not only go from the usability of the system by the user but also from the prediction of user action. When a person designs such a system, it is essential to understand what and how project elements would affect user action [22].

Finally, it is essential to remember that such projects are built for target users, so they must be tested and fixed based on users' evaluation at different stages of development. The main idea is that the application must work in the user's hands, as planned in documentation [22].

2.3 Training techniques

After discussing the main topic and choosing the approach that would be used for training creation, need to think about the training methodology. When a person teaches

something, he uses methods or techniques that provide content in a specific format, like text, speaking, or practical training.

Conventional Method - training method includes traditional teaching material about a specific topic [13]. This training method could consist of learning materials from text, slideshows, videos, or on-site with experts in the field [6]. The advantage of this training method is that a person who learns material could learn it in the order that he likes and in different ways. Also, when someone teaches about a topic, the person could ask for additional information if he has a question. The disadvantage of this method is that the person who learns this information receives only knowledge about the topic, not practical skills. Also, it is not a fact that the person who learns the topic is interested in it, and because of that, he forgets the information he was provided quickly. In a situation with an expert, it is also important that the expert is interested in teaching by providing information to students, and students are interested in the topic by asking questions.

Game-based Training - training provides material about the topic in game format. For example, board games have different cards about phishing scams, and player need to use cards from another deck with answers on how to react [6, 13]. This training method could use different types of games, such as computer games, board games, ARG, etc. It could be loaded to the internet as a web game or software that the person installs on his workstation. [13]. The advantage of this format is that a person who likes the topic receives knowledge and practical skills. Also, this type of game is more accessible and has different formats, which gives a choice of how a person would receive information about the area in which he is interested. As a disadvantage, creating a game needs a lot of work and effort, and as complex a game is, the more recourse it would take for its creation. Also, because of the game's complexity, some features could not be interesting to the audience for which it was developed, and because of that, all work could go into the trash.

Online and Software-based - training method which provides information about the topics in an online format or by using software with provided topics [6, 13]. For example, when a person learns something new from the course on the platform and receives knowledge and skills about a specific topic by provided materials on the course. Because this training method uses the internet as a delivery source, it is open to every person. If we talk about the advantages and disadvantages, they are the same as the Conventional training methods. They could be different based on which content is provided by a person who creates training and how it is delivered in training.

Simulation and virtualization based - taring which simulates the situation on provide data.[6, 13]. For example, applications have information about different cyberattacks; for example, let it be Spear Phishing. When the person needs to train in this topic, the application generates a scenario based on this attack from its data. This type of training provides a person with practical skills. Also, if this scenario is based on real events, he

would know what he could do if he faces the same cyberattack. Because cybersecurity always finds new vulnerabilities, it is important to update the database of such training programs. Also, the person must know the topic, which will be trained by this method.

2.4 Gamification

In section 2.3, different training techniques were described. From them were chosen gamification techniques because of the opportunity to provide content in many other formats such as video, audio, and through interaction, which also gives practical skills. The second reason is because of the human-centric approach to creating training, which could be interesting for the different sides that need to provide the target audience with content in a suitable format, and gamification provides this opportunity.

Games are complex media that require knowledge about where, how, and in which type of content developer would provide for the target audience. To better understand later research and how training would be provided in game format, lest discuss its elements.

2.4.1 Types of games

First, we need to figure out how people play games and how developers deliver content to the users. For that, need to choose a type of game that would be a game's core and build around it game mechanics.

Board games - tabletop games involving two or more players in the competition. The players move or place pieces or pre-make playing surfaces. A board game contains dice, cards, or tokens representing the different players. It could also include various items representing currency, points, or other elements used in-game mechanics [34].

Card games - use a deck or pack of cards for the game. Cards could be unique or same in deck [34].

Computer games - are games on electronic devices such as a laptop, computer, or console in which the player interacts with in-game objects using a controller, joystick, keyboard, or motion-sensing device [34].

Escape room – is a game where a player or a team is locked in a room to escape it. They must solve a series of puzzles within a set amount of time to escape the room [34].

Virtual reality (VR) - VR games immerse players into a 3D virtual environment. It provides players interactivity through audio and visual images to give them the illusion of the real environment [34].

2.4.2 Game genres

Next, choosing a game genre that describes how a person would play a game and which mechanics are included is crucial.

Action genre – this type of game gives the player an adrenaline rush that keeps him always involved. This type of game requires hand-eye coordination and quick reflexes. An example of a cybersecurity game is a game that requires players to protect themselves against cyber-attacks, e.g., tower defense [34].

Role-playing genre – in this game, players are required to create characters for roles in a fictional setting and play these roles as they like. Role-playing games (RPG) provide the player the experience of developing and playing a functional role with all of the mechanics such as character growth; a story, which changes based on the players' decisions and growing challenges and complexity [34].

Simulation genre – This type of game creates a copy of the existing environment and provides a player role. The main difference between this type of game and an RPG is that a simulation game simulates an existing environment, and an RPG provides what fantasy creates. Also, in simulation games, players have already created roles instead of giving players tools for making their own characters, as in RPG games. Simulation games use physical, mathematical, or logical models to create an environment similar to the existing one [34].

Adventure genre – this type of game has a storyline mainly concentrated on exploration. For example, the player could have work in the organization, and in one day, there is a change in the system, and the player participates in recovery operations [34].

Sports genre – this type of game requires a team of necessary player count and assigning roles to each member for doing specific tasks for the team's win [34].

Casual genre – this type of game is easy to learn and master. They are mostly video game versions of a board, card, or phone game. Each play session starts a new game, sessions do not continue from a previous one. As an example of a cybersecurity game, the user could have a small task related to connecting to the right router or providing the right command [34].

Capture the flag (CTF) genre – this type of game sets players or groups against each other to test their ability to find specific information with their skills. Typically, this information is a flag as an indicator that they used the correct method to pass particular tasks. An example of such a game is cybersecurity challenges, where the player needs to use their knowledge in Windows or Linux to find flags on the platform [34].

2.4.3 Game mechanics

Games can be deconstructed into different elements as one type of content provider. Some of these elements create experiences, emotions, or ideas that the users could think about later. These elements are named mechanics and explain how a person would play the game.

Conflict – mechanic gives the player the task to conquer or defeat the enemy by providing specific tasks. These tasks could be an obstacle to overcome, combat with another player, or a puzzle to solve [34].

Strategy and chance – strategy requires the player to think about how he would use specific gameplay elements in his favor. For example, when a player has to move a unit somewhere on the map, he needs to think about which way would be better. That person pays attention to specific details of the game, which helps him achieve his goal in the game [34].

Aesthetics – the game should look appealing to the player. The game's visuals can capture a player's attention and immerse them in the game [34].

Theme and story – themes contain the game's subject matter and connect the game with the player. They provide the game's background story and are usually included in the rules. The story provides a narrative throughout the game, which is helpful for players to not remember every fact from the story if the narrative is built logically. Instead of facts that are out of context [34].

Rewards – are things a player earns from achieving or accomplishing specific tasks in a game. Rewards such as points and badges boost player interest in the game [34].

Mystery – such element hides information about the story or world of the play, which makes him interested in digging into something unknown. Players should be aware of this gap and search for information to fill this gap in their knowledge about specific story elements [34].

Challenge – the game should challenge the players at every opportunity. Need to remember to provide appropriate difficulty that player could pass game [34].

Penalty – is the opposite of reward. Players should be required to start afresh or lose points due to wrong decisions. When the game has stakes, it brings the player to a more cautious gameplay, which helps to create interest in the game [34].

The opportunity of mastery – a game should give the player the opportunity to master the subject matter. The game should show that by progressing through it, the player will receive an experience that would be transformed into a new way of playing, and by that, the player creates interest in it [34].

Visibility of progress – the game should give the player feedback on his performance. When the player sees his progress and how effectively he passed through the level by seeing someone else result, he understands that he still has something to learn [34].

Emotional content – the game should bring out the human emotions in the player, such as frustration, excitement, anger, happiness, sadness, and joy. By showing emotions, the player creates a link in his brain with the game. If he needs to feel this emotion again, he will play this game [34].

2.4.4 Gamification frameworks

As was said in section 2.4, games are complex media that require to provide specific content for specific auditory. Because of that, games need to be analyzed from different sides so that the developer knows which elements add to the game, that the target audience would be happy about the product, and that the developer's main idea behind the game

would be interesting to the audience. For that, different gamification frameworks were developed for the analysis of games from various sides and to create plans to integrate content.

SETA - cybersecurity tools and security education training and awareness. This framework is concentrated on raising cybersecurity awareness among different types of people by providing questions about situations that could happen in practice and measuring them by points. Also, this framework requires a survey after task completion to better understand how well the program is created [36, 2].

EMERGO - framework concentrated on providing a simulated environment for the user to solve real-life scenarios in real-time. Such a framework creates simulation scenarios that are as close to real life as possible for better practice [36, 31, 31].

Octalysis - a framework that divided human drive into eight different sections: Epic Meaning and Calling, Development and Accomplishment, Empowerment of Creativity and Feedback, Ownership and Possession, Social Influence and Relatedness, Scarcity and Impatience, Unpredictability and Curiosity, Loss and Avoidance. Because a game could play different people with different mindsets, such a framework helps create the proper anchors, which would drive users into the game [36, 30, 23].

MDA - a set of rules used to psychologically drive the user (Aesthetics (A)) to act (Dynamics (D)) by using mechanics which the game includes (Mechanics (M)). It uses a set of familiar mechanics and rewards that interest the user in playing the game, such as points, levels, challenges, rewards, status, and accomplishment [36, 30].

MDE - provide the same principle as MDA. It concentrates not on engaging the user to action but on providing the right emotions [36].

6D - framework which helps in game creation following six steps: Define Business Objectives, Delineate target behavior, Describe your players, Devise activity loops, Don't forget the fun, Deploy appropriate tools [36, 33].

As you can see, cybersecurity has different gamification frameworks that help to narrow the right path for game creation. These frameworks have different ideas about how games should work and give results based on their ideas. The main criteria for choosing the framework are: (i) the game should work together with human-centric aspect ideas, (ii) it should interest the user in the process of learning new things from the game, (iii) it should work with the target group, and (iv) it related to computer game creation. Table 2 on page 34 provides an analysis of frameworks.

Framework	Human-centric	Target group	Interest in learning	Computer game
SETA	yes	yes	no	yes
EMERGO	no	no	yes	yes
Octalysis	yes	yes	yes	yes
MDA	no	yes	yes	yes
MDE	no	yes	yes	no
6D	no	yes	no	yes

Table 2. Frameworks analysis

A suitable framework for game creation for this thesis is Octalysis. Octalysis's main principle is based on the human-centric aspect, where the system is built around user needs. Because this framework provides analysis from different sides of how users are interested in the product, this helps create an interesting game for different people. Also, it help to change the game in the future because of the various parameters that Octalysis uses for analysis.

2.5 Summary

In this section, we provided information about each topic used in training program creation in Section 5. We discussed social engineering, which techniques it uses, and how. Covered human-aspects work principles, approach, and how it is designed for the user. Which types of training could be used to educate a person? The training was chosen for game-based training due to its variety of ways to provide content for the audience and the use of practical exercises. Discussed different types of games and related to their genres and mechanics. Also, gamification frameworks were discussed, which helps analyze the game core. The training was chosen by the Octalysis framework because of its human-centric approach to analyzing user needs in products and various parameters for analysis.

3 Research Protocol

This section provides information about the research process, including social engineering techniques used in research, the process of receiving data for later study, and additional information about topics that needed to describe the research process.

3.1 Selection of social engineering techniques

In section 2.1, different techniques were described that are used in social engineering attacks. Some of them use skills that require a deeper understanding of human psychology than technical or more technical skills related to computer science, such as computer engineering or programming knowledge. Because our target group is 10-12 classes of school students, there is little chance that someone has deep knowledge about the topics provided earlier. Because of that, one of the criteria for social engineering techniques that are used for training is that they do not require deep knowledge of technical skills in areas beyond regular school programs. Training requires students to use skills in analyzing provided information and creating logical steps to mitigate social engineering attacks. Also, social engineering techniques need practical use on the target group and be related to using electronic devices such as computers or phones. The analysis can be found in Table 3 on page 35.

Social engineering techniques	**Require analytical skills**	**Related to target group**	**Use of computer or phone**
Phishing	yes	yes	yes
Vishing	yes	yes	yes
Smishing	yes	yes	yes
Spear Phishing	yes	yes	yes
Angler phishing	yes	yes	yes
"Evil Twin" WIFI or WiPhishing	yes	yes	yes
QRishing	yes	yes	yes
Pretexting	yes	yes	yes
Grooming	yes	yes	yes
Profile cloning	yes	yes	yes
Shoulder surfing	yes	yes	no
Quid pro quo attack	yes	yes	yes
Dumpster diving attack	yes	yes	yes
File masquerade	yes	yes	yes
Scareware or Pop-up window	yes	yes	yes
Deep fakes	yes	yes	yes
Whaling	yes	no	yes
Face-to-face interaction	yes	yes	no
Diversion theft attack	no	yes	no
Water-Holing	no	yes	no
Tailgating	no	no	yes

Table 3. Analysis of social engineering techniques

The following paragraphs provide an overview of selected social engineering tech-

niques, explaining why they are relevant for this audience and how understanding them can enhance their cybersecurity awareness.

Phishing, Vishing, Smishing, Spear Phishing, Angler Phishing, "Evil Twin" WIFI (WiPhishing), and QRishing are various phishing attacks. These techniques rely on psychological manipulation rather than technical skills to reveal the target's personal information. Teaching students these techniques helps them recognize and avoid common traps, safeguarding their personal information using psychological manipulation.

Pretexting, Grooming, Profile cloning, Quid pro quo attacks, Dumpster diving attacks, Scareware or Pop-up windows, File Masquerade, and Deepfakes are attacks under all conditions. To mitigate such attacks, a person uses their analytical skills to understand if he is attacked. Also, these attacks are related to our target group not only because this target group is school students but also because these attacks are related to technology that our target audience uses, such as computers or smartphones.

For Grooming, Pretexting, and Profile cloning techniques, use social media platforms such as Facebook or X(Twitter) for posting information, which could be used to manipulate person or platforms for online communication such as Telegram or WhatsApp, which is used by the target audience for communication with their friends or family. It creates danger for the target group because they use such platforms where these attacks could happen.

Quid pro quo attacks, dumpster diving attacks, file masquerades, and deepfakes play on the trust of a specific person, group, or service or do not manage their personal data well. Because these attacks affect people's confidence, checking whether the target group trusts another person's personal information is important.

Scareware or Pop-up window attacks use Pop-ups that have malicious links. These attacks are old but still used by attackers. These attacks are suitable for training because they do not require knowledge of technical skills but only analytical skills.

Specific social engineering attacks have been excluded from the educational game due to their particular targets, context, or the level of technical knowledge required to understand and mitigate them. For example, (i) a whaling attack is not concentrated on high school students but mostly on high executives of organizations. Therefore, including this topic would not significantly benefit their understanding of social engineering threats relevant to their age group. (ii) Face-to-face interaction attacks do not align with the digital context the game aims to address, making it less relevant for inclusion. (iii) Diversion Theft Attack is logistical and operational, focusing on the physical movement of goods rather than digital or psychological manipulation. High school students are unlikely to be involved in scenarios where they manage or handle corporate logistics, making this attack less applicable to their experiences. Consequently, it does not serve the educational goals of the game. (iv) Mitigating such attacks as Water-Holing often requires advanced technical skills, including web security expertise and the ability to analyze and secure network traffic. Given the technical complexity and the need for

specialized knowledge, this topic is beyond the scope of what high school students are expected to understand. Focusing on more accessible social engineering techniques is more beneficial for this audience. Moreover, (v) Tailgating exploits human timidity and the physical access controls of an organization. Since Tailgating primarily concerns physical security within organization premises, it is not directly relevant to the digital and online security context the game aims to address. High school students are more likely to benefit from learning about social engineering tactics that affect their personal digital security rather than corporate physical security practices.

3.2 Design and implementation of two-phase testing protocol

The testing process comprises two phases. The first testing phase gathers data on current knowledge and skills in social engineering. The second phase begins after the applicants from the first phase go through a training program created using collected data. The second phase tests applicants' knowledge from the first phase and compares the first and second phase results to understand how the training program was effective. In the first testing phase, we selected two schools from Ida-Viru county.

- Narva Eesti Gümnaasium
- Narva Kesklinna Gümnaasium

We specifically chose Ida-Virumaa as a region for the research and testing of new teaching methods because of the world's current geopolitical situation. In 2022, the Russian government started the war in Ukraine, which increased warnings about the defense of European countries against the military activity of Russia. This conflict raises questions in the European community on how much Europe is prepared against probable cyber threats such as attacks on critical infrastructure or social manipulation. Next, arguments are provided for why the Ida-Virumaa region was chosen for research and how it is connected with what was said earlier. For example, years earlier, several groups with connections with the Russian government or people from Russia had already done cyberattacks targeting systems related to elections and campaigns to manipulate public opinion. For example, in 2020, two Russian pranksters broke into the security system for telephone calls from the President of the Republic and talked with him for 11 minutes. Using social engineering techniques, they asked him different provocations questions about the current situation with monuments related to the Soviet Union solder heroism against Nazi occupation in Europe and the current relationship with the Ukraine government [12]. As another example, in 2017, Russian hacking group APT28 tried to infiltrate the German foreign and defense ministries by using malware [8].

Additionally, Ida-Virumaa is the border region with Russia, and in its region, most people speak the Russian language. According to information from the INTERNA-

TIONAL CENTRE FOR DEFENCE AND SECURITY report of Estonia, Russian-speaking people in Ida-Virumaa is 96% [15]. This creates a situation where the region could be used as the target of a massive social engineering attack against the current political system, which the Russian government does not like, or create misinformation that could cause a bad situation in the region.

3.3 Phase-I questionnaire

The first questionnaire is created to collect information on decisions made when the target of a cyberattack is the respondent. From a cybersecurity standards perspective, these responses will be checked and evaluated based on whether the respondent's action is dangerous or safe. Because some topics are related to cyber hygiene, such as Dumpster diving, those topics use questions about cyber hygiene.

This questionnaire was validated by MSc Mari Seeba on 12.01.2024 in the format of a Skype conversation. In conversation, we discussed questions created for the questionnaire, how to develop questions for a questionnaire that could be understandable for the target group, and which questions give accurate data.

3.4 Phase-II questionnaire

A second questionnaire checks what 10-12 class school students learned by passing the created training program. The second questionnaire checks high school students who did the first questionnaire to see how their knowledge and skills changed after passing the training program. Questions created in this questionnaire are based on social engineering techniques used in the training program. This questionnaire use the same methodology as the first to understand how actions in specific situations when dealing with social engineering attacks differ before passing the training program.

3.5 Consent form

A consent form is a document that gives information about data collected by research, how it would be used, and by whom it would go under GDPR rules. This consent form was created by Santeri Pohjaranta and was checked by Terje Maesalu and the supervisor. A consent form copy can be found at GitHub repository[3]. The questionnaire would last approximately 15 minutes, and the person who pass it could drop it at any time. As was said earlier in 4 and 6, this questionnaire would collect personal actions in situations with specific social engineering techniques. Personal data collected from the user would be age, class in school, gender, and email.

[3] https://github.com/santeri13/SEEG

3.6 Pilot study

A pilot study was conducted to check how well the target group understood the questions in the first questionnaire and what answers could be given. For the pilot study, was asked to pass a questionnaire by the same age group as in 10-12 classes. Based on the questionnaire results, some questions were changed, primarily related to collecting personal data and some questions related to social engineering.

3.7 Summary

This section prepares the material required to receive data to answer research question SRQ1 and provide data for training creation. It covers an analysis of relevant social engineering techniques for questionnaire and training program. Describe how data is received by using the two-phase testing protocol. This protocol covers two questionnaires that show changes in social engineering knowledge and skills among high school students. Also, a pilot study for questionnaires was conducted to understand if questionnaires provide data in a suitable format for research.

4 Results of Phase-I Questionnaire

This section provides the results of the first questionnaire and answers to the SRQ1 question from Section 1.2. The results are evaluated by the responses the respondents gave. Because the main idea behind testing is to see which topics high school students lack knowledge and skills, the results analyzed by sex and grade in school and from which school the results were received. As was said earlier, questions could have one or multiple answers, or the respondent could answer the question himself. Answers to questions are provided in graphs with detailed descriptions and discussions on each question. Results, where respondents must write answers themselves, are described separately without graphs.

4.1 Demographics

First, let us discuss data about respondents to provide information on which group we work with in this research. Information is seen in questions 1 - 5 (see Fig. 21 - Fig. 25). For this research, information was collected about respondents age, gender, study level in school, and the school in which they learned at the moment of data gathering. Also, information was collected about their preferences in sharing personal information on the internet to see which kind of data could be in danger if respondents have problems with any social engineering technique. By answers to questions 1-3 (see Fig. 21 - Fig. 23), our group is 15 - 20 years old, has a balance in gender, and is mostly in 11, 12 classes by study level. By data from question 4 (see Fig. 24), information which our group shared on the internet are name, age, email, phone number, and social networks such as links on their Facebook or X (Twitter). This is understandable because young people try to find new contacts using existing technology and use information by which they could be identified. But they do not put information by which their living place could identify them. This supports question 4 (see Fig. 24), where it could be seen that respondents do not share their home addresses. This shows their caution about sharing specific information by which they could be stalked.

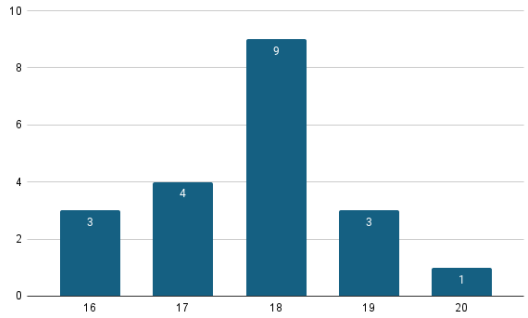

Figure 21. 1. What is your age?

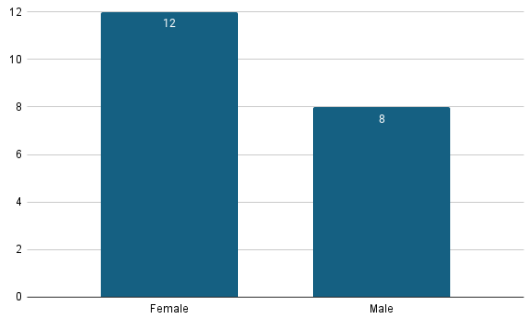

Figure 22. 2. What is your gender?

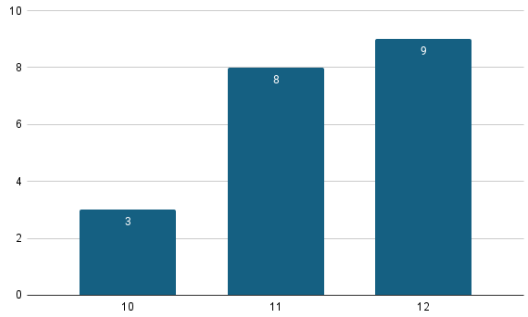

Figure 23. 3. What is your school study level?

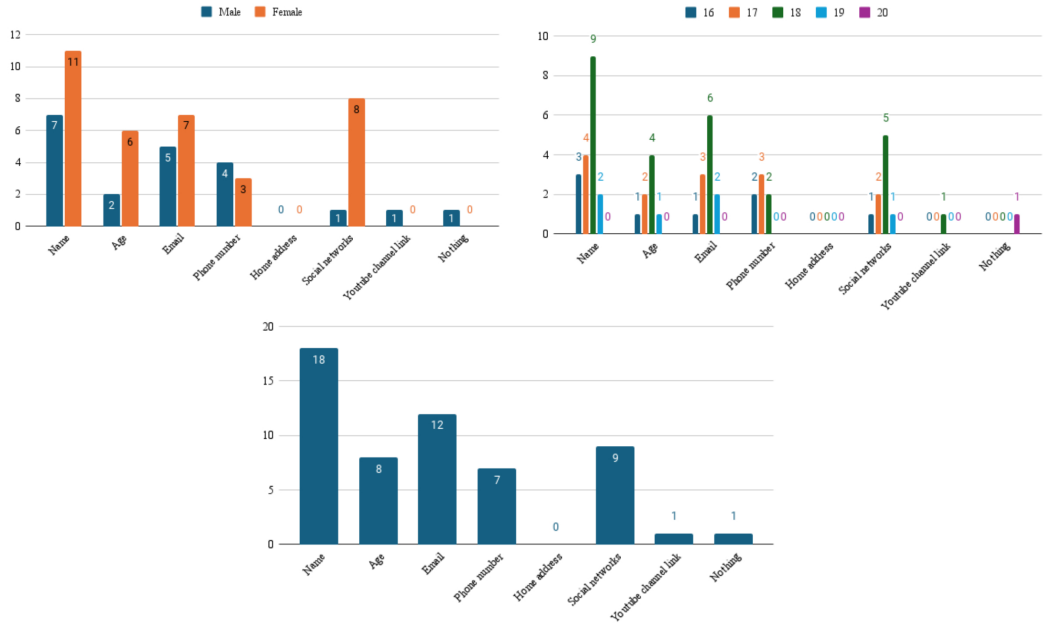

Figure 24. 4. How much personal information do you write on the internet?

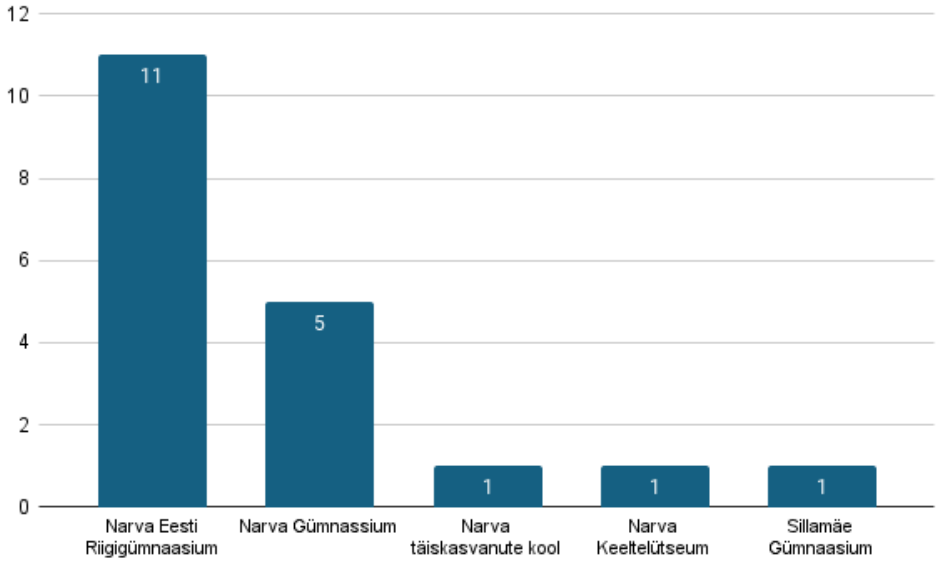

Figure 25. 5. In which school you study?

4.2 Knowledge of social engineering techniques

Next, let us discuss respondents knowledge of social engineering techniques. According to data from question 8 (see Fig. 26), most respondents know about Deepfakes and a little about Email Phishing, Face-to-face, Scareware, or Pop-up windows. Next on the list are Profile Cloning, File Masquerade, and Evil Twin WIFI. Deepfakes have been popular on the internet in the last few years, and understandably, school students know about them. We receive interesting results when we go to Email Phishing and Scareware or Pop-up windows. They are one of the oldest social engineering techniques, and, interestingly, they are not on the same level as Deepfake. One of the theories why they are not well known is that they are old and familiar techniques. Because of that, people know that such a technique exists but do not know the official name of it. If we compare Deepfake with Email Phishing, then Deepfake is a young technique that has been used recently. Because of that, school students have heard and know a lot about it. The second theory of why Deepfake is more popular is that this technique is used in creating audio and visual content. Young people who are also school students like to make creative content, so they could use software that adds Deepfake images or videos and post them to others. When other people see it and find out that it is not real but are interested in trying something similar, they find out information about Deepfake. The third theory could be not knowing the terminology of social engineering techniques. If describing written answers in question 7, respondents wrote that they do not know about anything; it is related to fraud and, receiving personal information, manipulating people to perform specific actions. Most respondents do not know anything about social engineering.

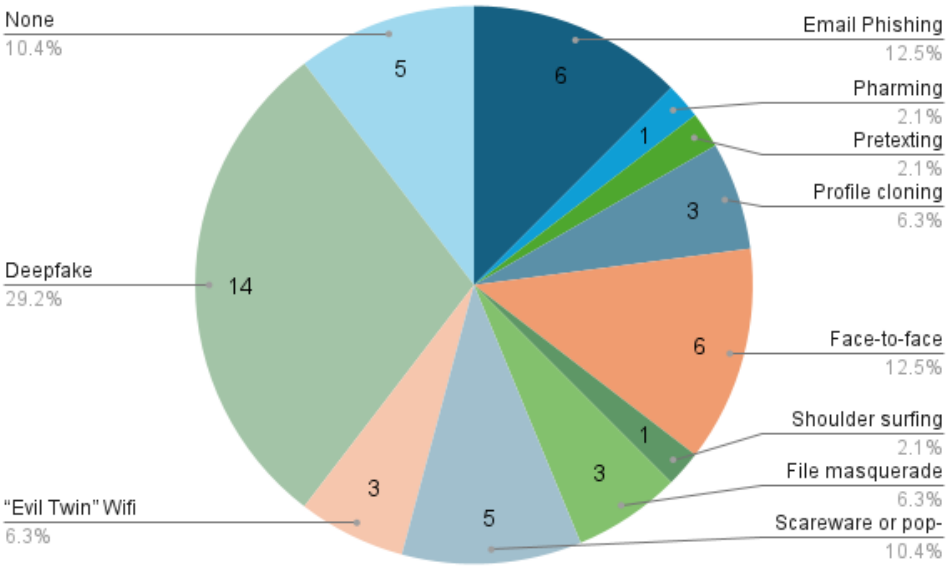

Figure 26. 8. Do you know any social engineering methods from these?

4.3 Skills against social engineering techniques

The following questions are related to respondents' skills in mitigating social engineering techniques. The first is questions related to cyber hygiene. These questions were created for the Dumpster diving attack technique. Because this technique concentrates on using gathered data, it is essential to understand how users are cautious with their existing and old data. If we discuss results in the Dumpster diving attack technique field, then from the questions, it is understandable that in most cases, respondents delete files and information not required for personal use. This indicates that respondents are less vulnerable to such a technique. If we discuss results separately from the Dumpster diving attack technique, then by results from question 11 (see Fig. 29), most respondents keep their password the same for a while. This could indicate less interest in the safety of their data. But if check results in which period respondents do deep cleaning of their device from question 9 (see Fig. 27), then most of the respondents do this 1 or 2-month period. This shows that respondents are interested in cleaning their old data, which they do not use. The theory of why respondents clean their old data recently rather than change their account password for better protection in some periods comes from laziness. When someone works on their workstation, they only need to open a specific folder or see the file they do not use and delete it permanently. To change passwords on their accounts, they need to take more steps. As proof of this theory results from question 10 (see Fig. 28), where they checked to see if they save their account information in programs for automatic

information saving, most responders said yes. Because this is simpler than remembering many different account credentials, respondents use such programs, which shows their laziness in remembering different account information.

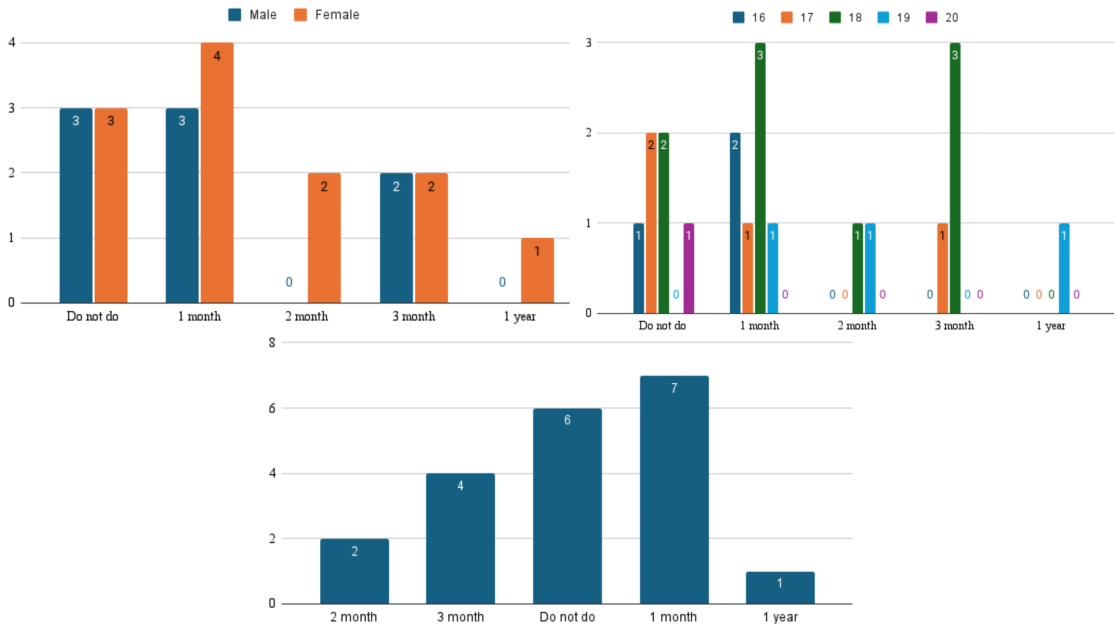

Figure 27. 9. In which period did you do deep cleaning of your device (clean your phone, laptop, and computer from old files)?

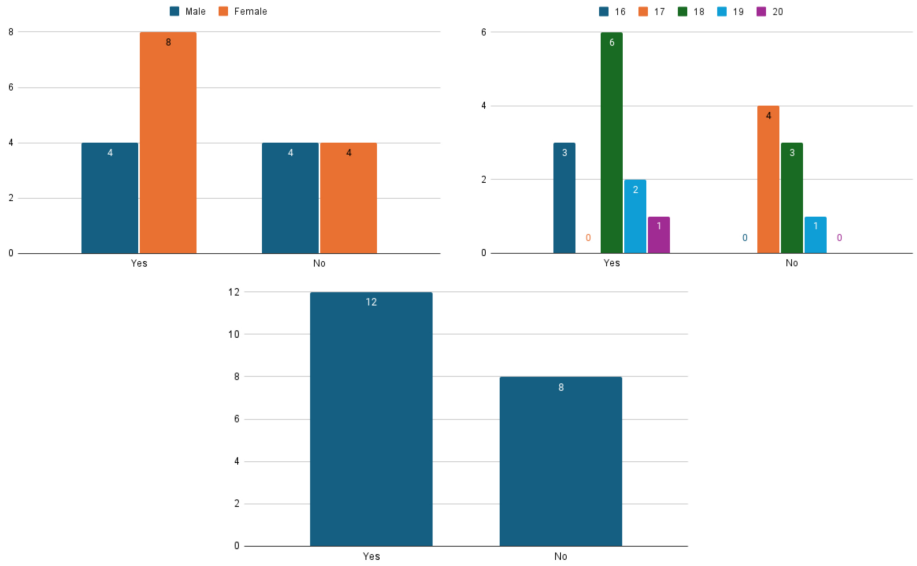

Figure 28. 10. Do you save your account information in programs for automatic information saving?

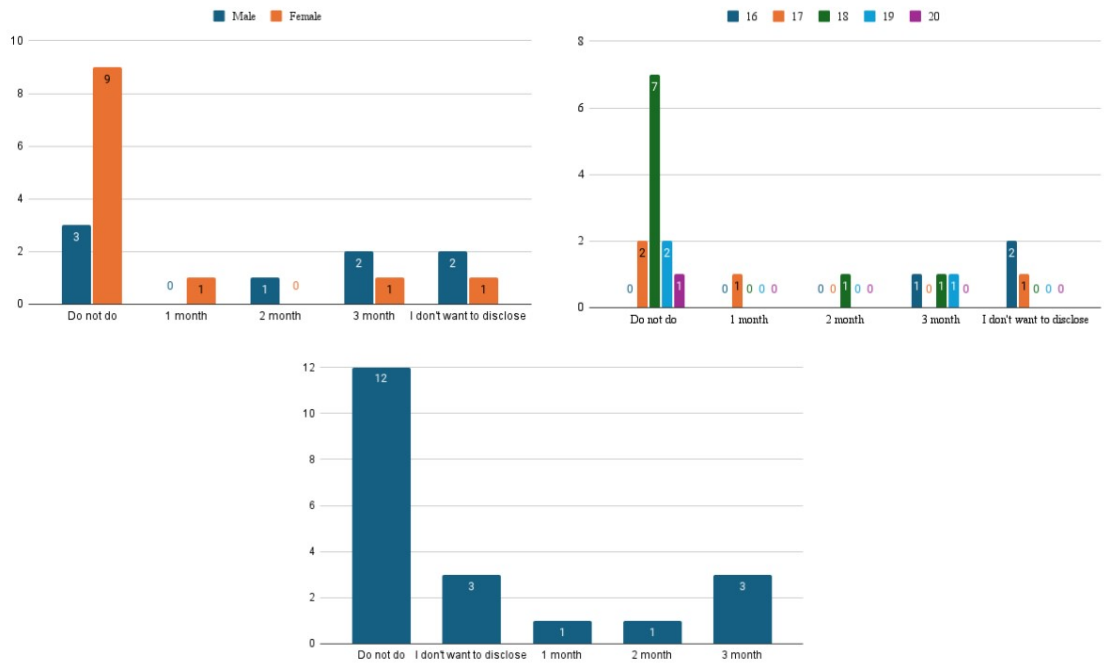

Figure 29. 11. In which period did you change your account passwords?

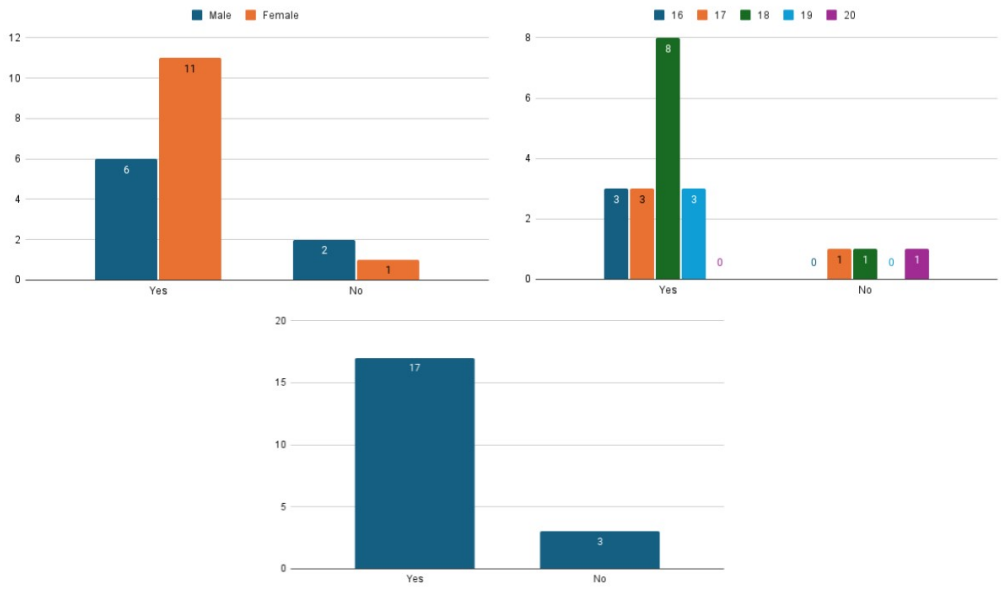

Figure 30. Question 12. When you delete some files do you additionally check if they are removed from the bucket?

The next question is related to Email Phishing. Questions from 13 - 14 (see Fig. 31 and Fig. 32) are created to check the respondent action when dealing with a particular situation. This is needed to check if a user is vulnerable to attacks that use information collection from the target or malicious software installed on a workstation by the user. According to the questionnaire results, such an attack could affect some respondents, but in most cases, respondents know how to deal with such attacks. If we take results from question 13 (see Fig. 31), which checked if respondents open files from email messages, then results are mixed. Respondents often check suspicious files or delete email messages; this could happen because they know the risks of opening suspicious files. But in some cases, they still open it. This could happen because of a lack of knowledge of such action risks. This theory proof can be seen in results from Fig. 31 on the age graph, where such actions by respondents from 16-17 years old. Question 14 (see Fig. 32) checked how the respondent would react if he received a message about his Facebook account being blocked, and to unblock it, he must go by the provided link. In this case, most respondents ignore such a message or delete it. Still, in some cases, respondents go by the provided link in the message. If we check Fig. 32, then we do not see any correlation of how to prove such action, but as a theory, this could happen because of a lack of knowledge of specific respondents.

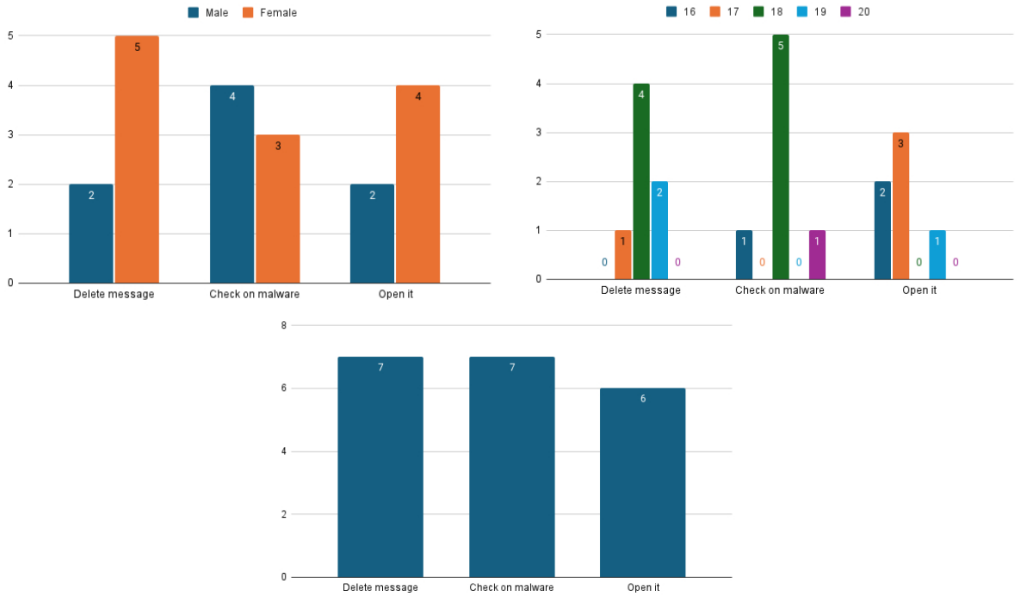

Figure 31. 13. You receive an email message with a file to open. What do you do?

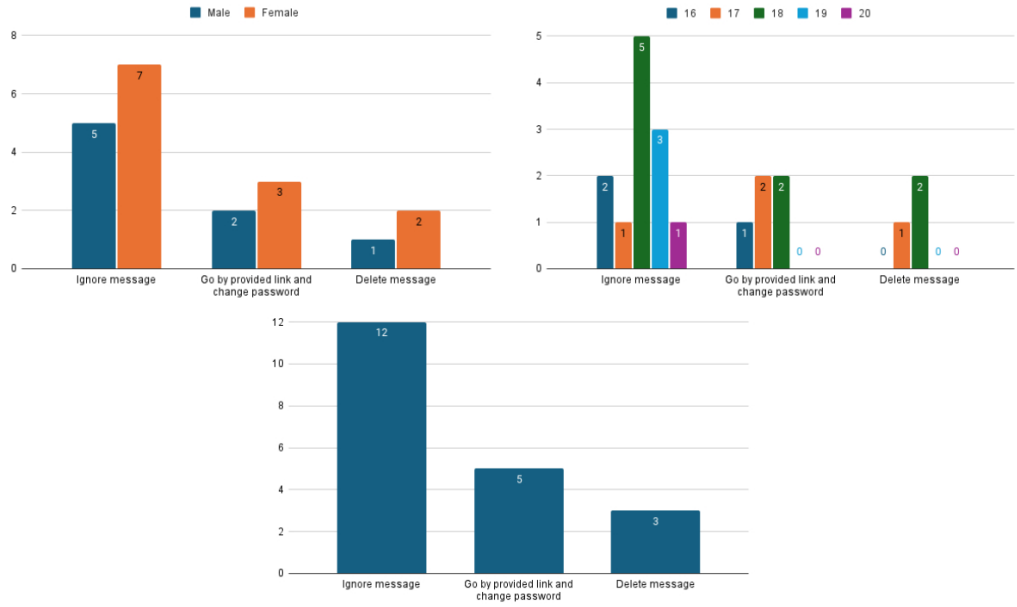

Figure 32. 14. You receive an email message that your Facebook account is blocked, and to unblock it, you need to go by the link and change your password. What do you do?

The questions 15-16 (see Fig. 33-Fig. 34) are related to Pharming. These questions are created to test what respondents would do when a attacker tried to receive credentials from their account and what respondents do if that was successful. According to results from question 15 (see Fig. 33), most respondents try to change their password on the same website if they think they have problems with credentials. According to our theory, this could come from not knowing Pharming techniques. Because of that, they are not aware that this could be an actual social media page. This theory could support the results of question 8 (see Fig. 26), where Pharming was known only for one person. According to results from question 16 (see Fig. 34) of 10 respondents, changes on their account without notice would trigger action, such as changing credentials. Such action could come from warning that their personal information, which is held on their account, is in danger.

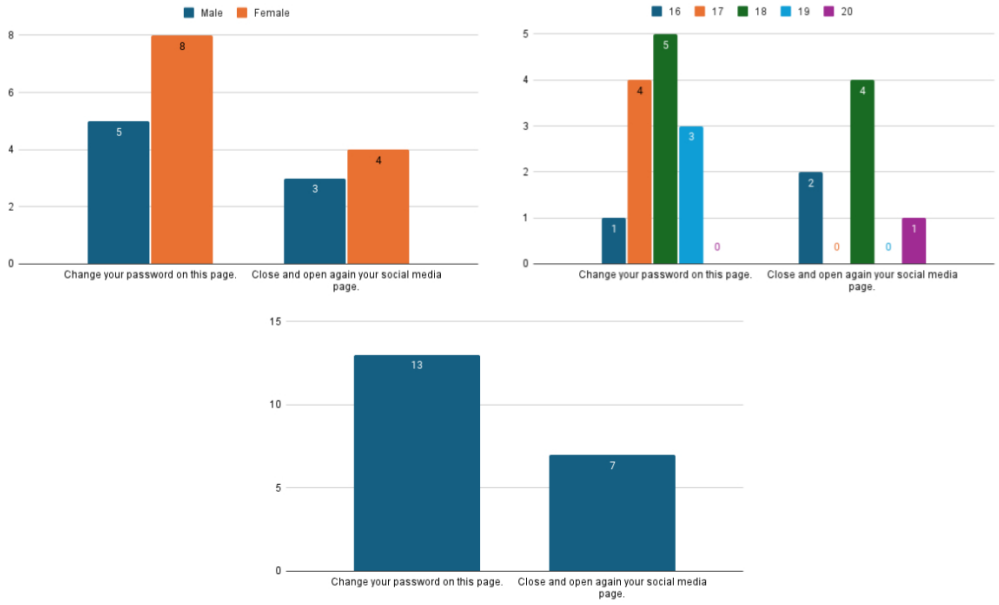

Figure 33. 15. You try to log in to your account on social media, but it says that your account information is wrong, but you know it is right. What do you do?

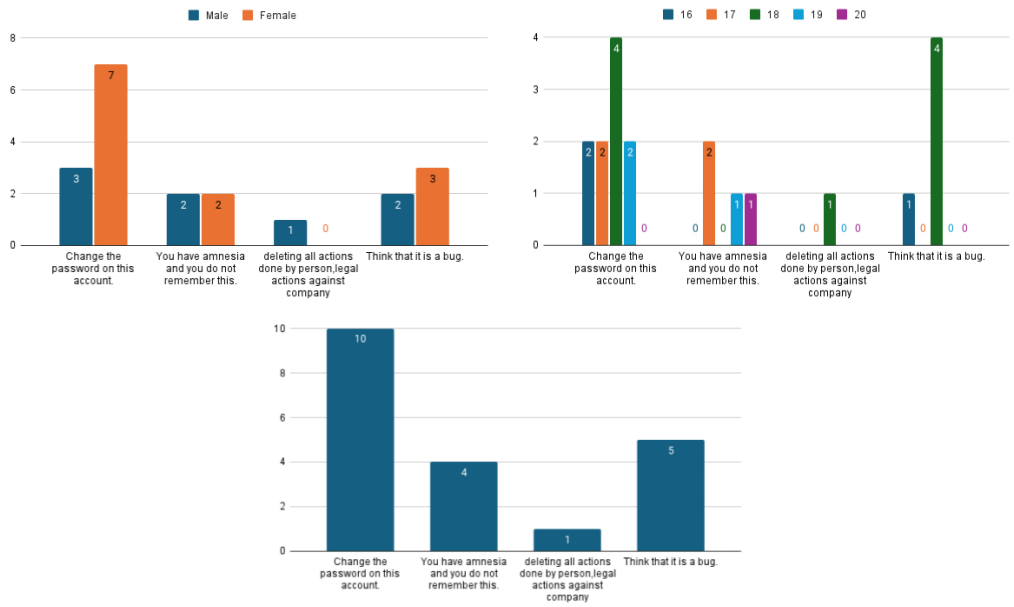

Figure 34. Question 16. You go to your social media page and see posts and friend requests that you have not sent. What do you do?

The questions 17-19 (see Fig. 35-Fig. 37) are related to Shoulder surfing. These questions were created to check respondents interest in essential data protection, when someone could see physically from a workstation screen, or when respondents give information themself. Questions 17 (see Fig. 35) and 18 (see Fig. 36) have multiple answers to see which actions respondents do. In question 17 (see Fig. 35), respondents mostly turn off their workstations when they need to go somewhere, which is partially the correct answer. If the workstations do not have a function to automatically log out from the account, or if they do not have a password, then an attacker could receive access to their workstation. Logging out from the account is a better action in such a situation. This answer is the second answer by popularity if check graphs in Fig. 35. Answers in question 18 (see Fig. 36) show that respondents delete their personal information when they deal with a situation when they need to provide a device to someone else where it holds their personal information. Answers in question 19 (see Fig. 37) show that almost all respondents stop someone when they try to see something important from the respondents devices. Answers to questions show that respondents are interested in the security of their information. As was said earlier, the Shoulder surfing technique is primitive, and to mitigate it, users only need not show their personal information to another person.

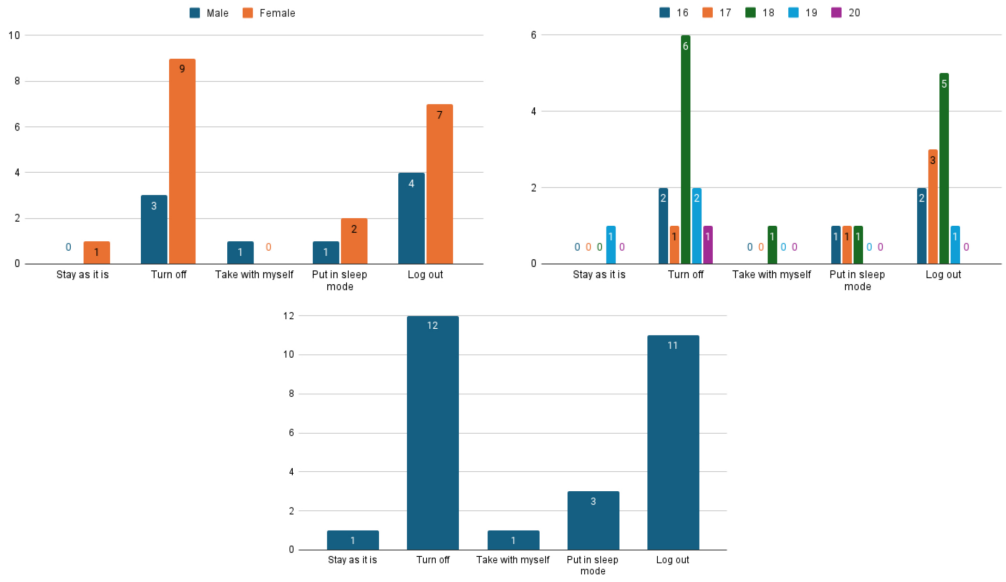

Figure 35. 17. You need to go somewhere else and leave your laptop/computer in the place where you worked. What do you do?

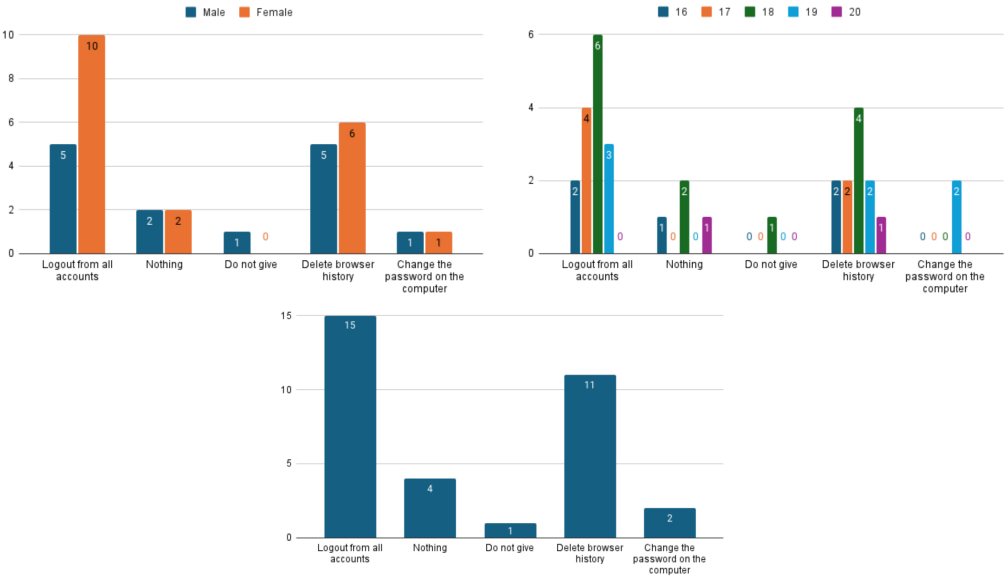

Figure 36. 18. You give your computer/laptop to check if something is wrong with it. What do you do?

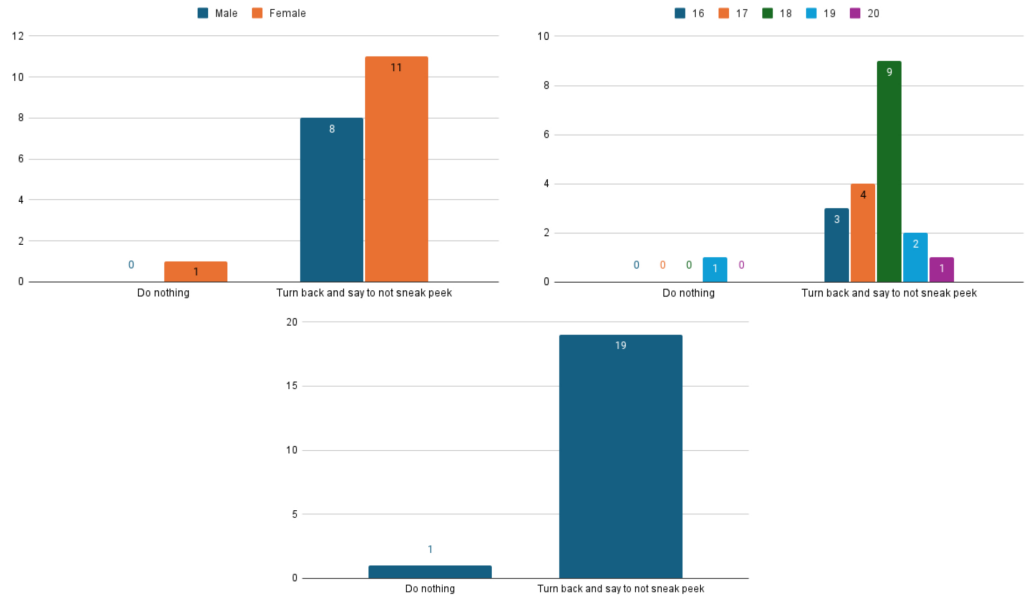

Figure 37. 19. You are working on your computer and feel that someone is sneaking behind your shoulder, what do you do?

Question 20 (see Fig. 38) was created for File mascaraed topic to understand if respondents figure out that problems with their workstations could happen because of programs they install. Results show that in most cases, respondents do a factory reset of their phone or check the app for malware if their phone glitches after installing it. This shows that respondents understand how dangerous it could be if they know that malware is on their devices. Some respondents said this is happening because their device is old. In theory, this could happen because of a lack of knowledge of malware and how it works. This could be supported by answers stating that this could happen because of malware. A person who knows what malware is and how it is dangerous will logically choose this answer.

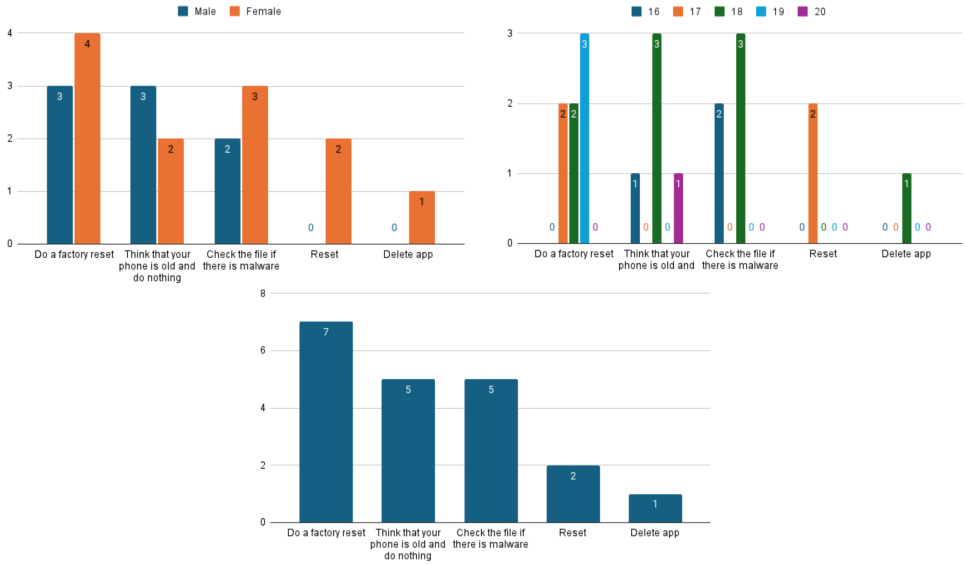

Figure 38. 20. After a little bit of application use, your phone starts to throw glitches. What do you do?

Question 21 (see Fig. 39) was created for Quid pro quo attack to see what users would do if someone who is not professional would work on their device. All respondents said they stay in place and see what the master would do. This could happen because respondents do not trust other people when dealing with their devices.

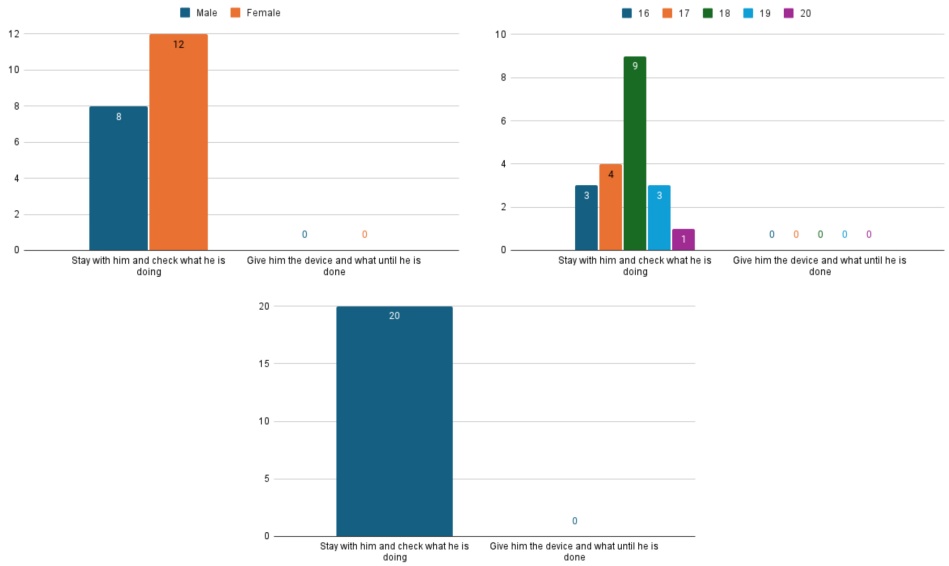

Figure 39. 21. You do not understand how specific functions in the application work and you give your device to another person to help with it. What do you do?

The question from 22 - 23 (see Fig. 40- Fig. 41) is related to the topic of Pretexting. This question checks respondents reactions to attackers who use fake personas to receive their personal information. Question 22 (see Fig. 40) all respondents reacted right when someone tried reviving their bank account access using social engineering. Question 23 (see Fig. 41) provided the correct reaction when the attacker attempts to receive access to personal data by impersonation a police officer. Answers to questions show that respondents understand how Pretexting works. Still, if we remember answers to question 8 (see Fig. 26), most do not know what it is. This creates the theory that even if respondents know about attacks, they are unfamiliar with the terminology.

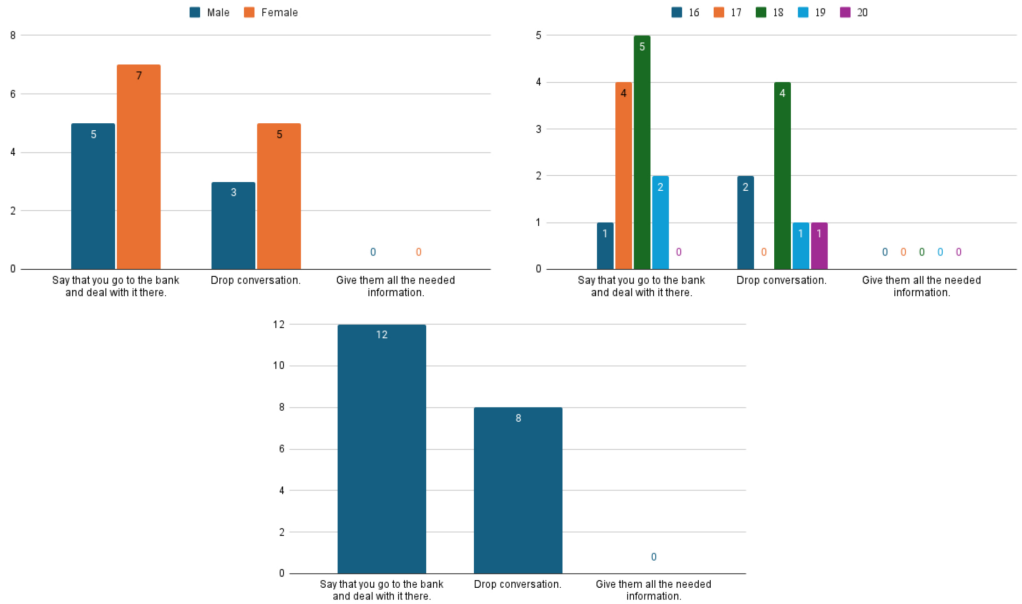

Figure 40. 22. A person from the bank phoned you. They say that someone is trying to steal money from your bank account and needs your personal information about your account to switch it to another account until they deal with the problem. How would you react?

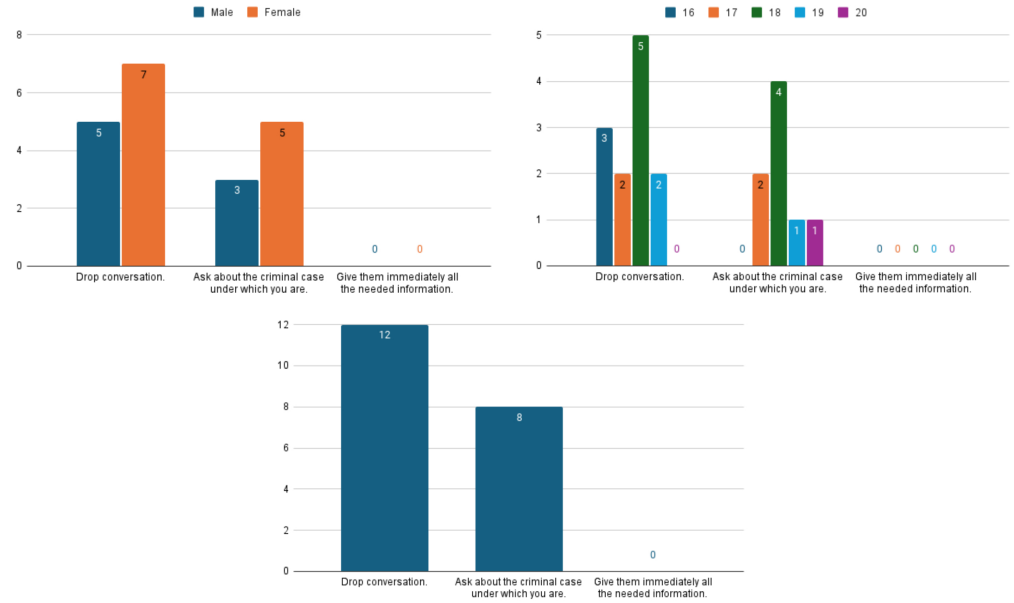

Figure 41. 23. A police officer calls you and says that you are under a criminal case and they need your personal information right now. What do you do?

The questions from 24 - 26 (see Fig. 42- Fig. 44) are related to Profile cloning. These questions are created to check how respondents would react when someone cloned their profile or used a cloned profile to manipulate the respondents. By questions 24 (see Fig. 42) and 26 (see Fig. 44), all respondents chose the right answer in the situation described in the questions. In question 25 (see Fig. 43), it could be seen that some respondents chose the answer "Think that it is a bug" when a friend received a message from the respondent, and he came to the respondent and asked if the respondent has written to him. As a theory, it could happen because they are not familiar with such an attack and have seen it for the first time. A proof of such theory questions 24 (see Fig. 42) and 26 (see Fig. 44), which also used the profile cloning technique, but the respondents chose the right answers. This shows that they understand how to deal with such a type of attack but not with the situation.

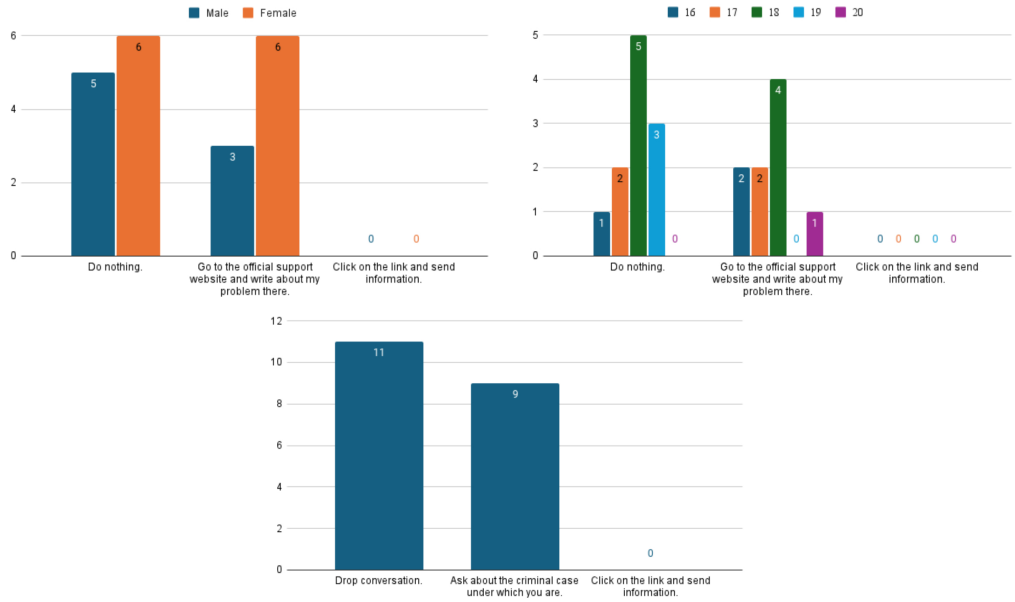

Figure 42. 24. You created a bad review on the product and received a message from support. He says that you can send information about problems to support by provided link to the form, what do you do?

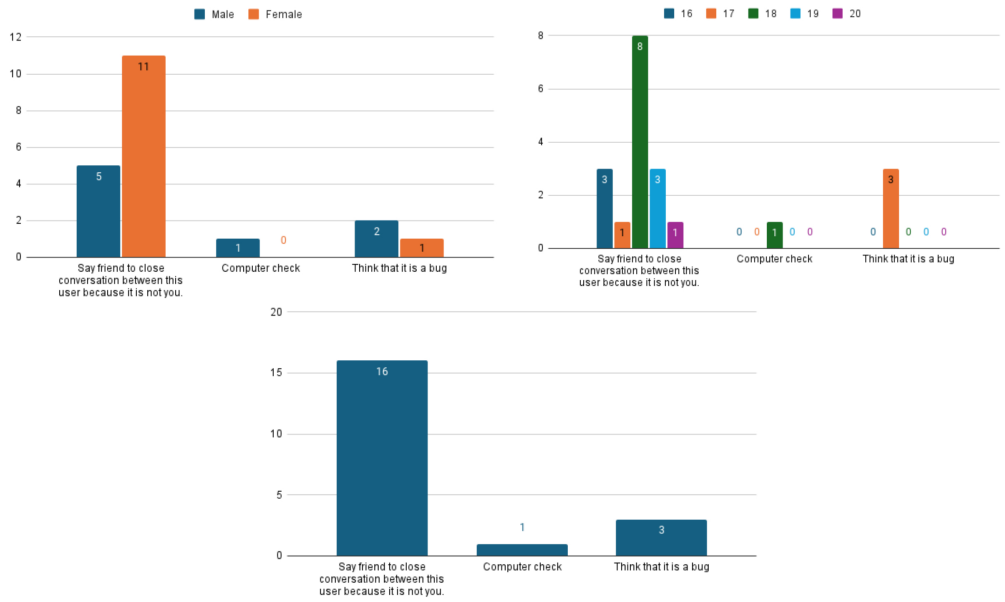

Figure 43. 25. Your friend receives a message from you, and he comes to you and asks if you have written to him when you are not, what do you do?

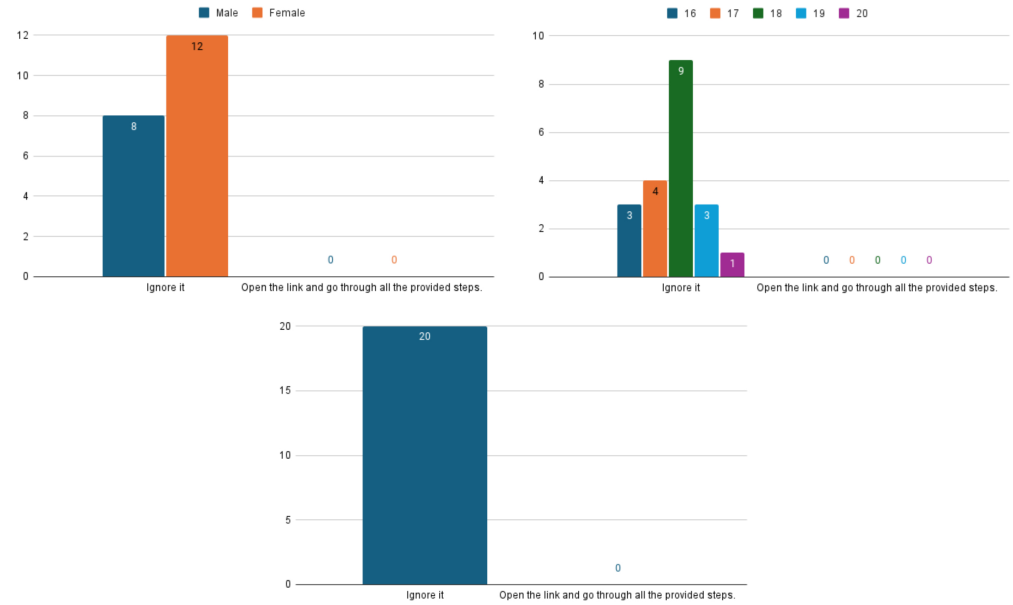

Figure 44. 26. A popular person from a telegram chat group sends a voice message that for activity check, you need to go by the provided link in YouTube and click on the like button on short. What do you do?

The questions from 27 - 28 (see Fig. 45- Fig. 46) are related to Scareware or Pop-up window. These questions are created to check the respondents reactions to Pop-up messages and what they would do with them. In question 27 (see Fig. 45), most respondents understood the risks of such a Pop-up message written in the questionnaire and did all right from a security perspective. In question 28 (see Fig. 46), more respondents opened malicious Pop-ups to receive prizes. This creates the theory that human manipulation has more chances of success if there is something valuable for a person.

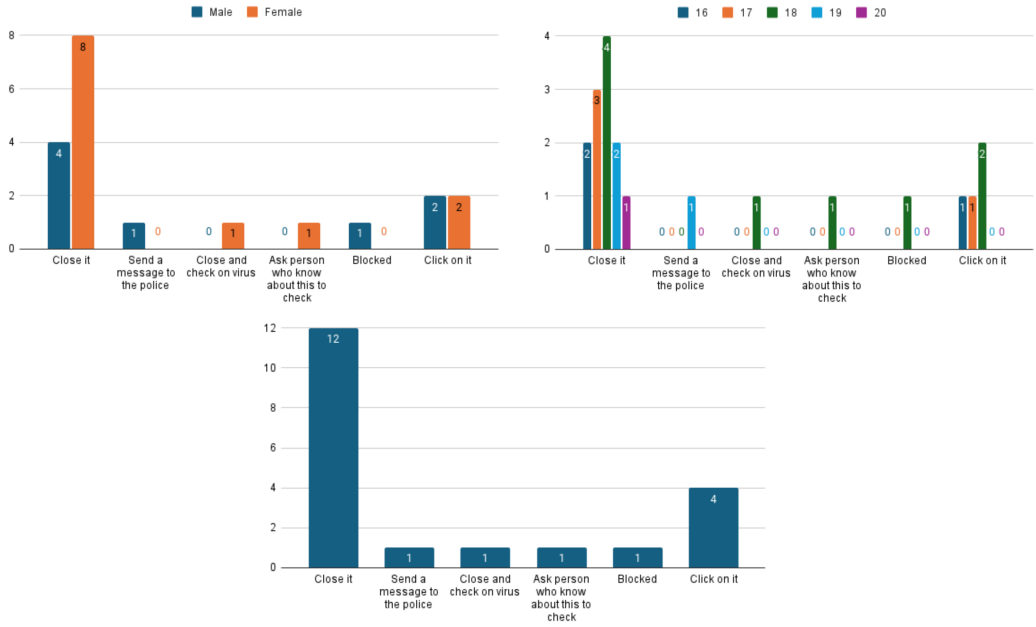

Figure 45. 27. You see a slide-in Pop-up message on a webpage that you have a virus on your computer. What do you do?

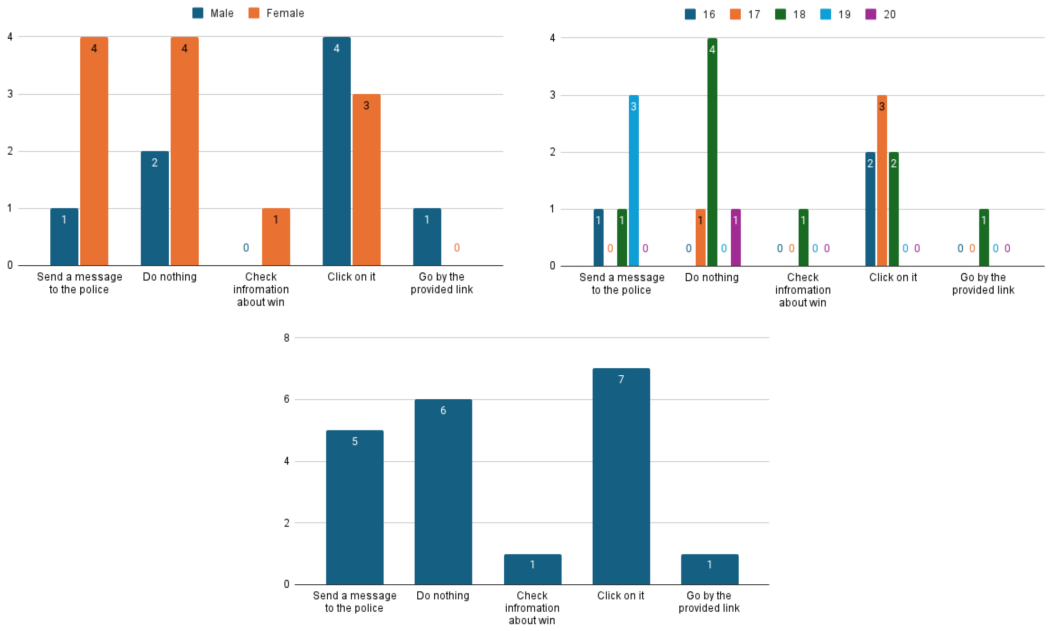

Figure 46. 28. You see a slide-in Pop-up message on a webpage that you won the price and need to redeem it. What do you do?

The question 29 (see Fig. 47) is related to Ewil Twin or WiPhishing topic. This question is created to determine whether respondents understand that connecting to public WIFI points could lead to loss of personal data. Most respondents answered that they would connect to public WIFI hotspots. From a security perspective, this is not good because respondents risk losing their data by checking packets in the network. Such an answer could come from a lack of knowledge about such techniques as WiPhishing. This theory could support question 8 (see Fig. 26), where Ewil Twin or WiPhishing knows very little from respondents.

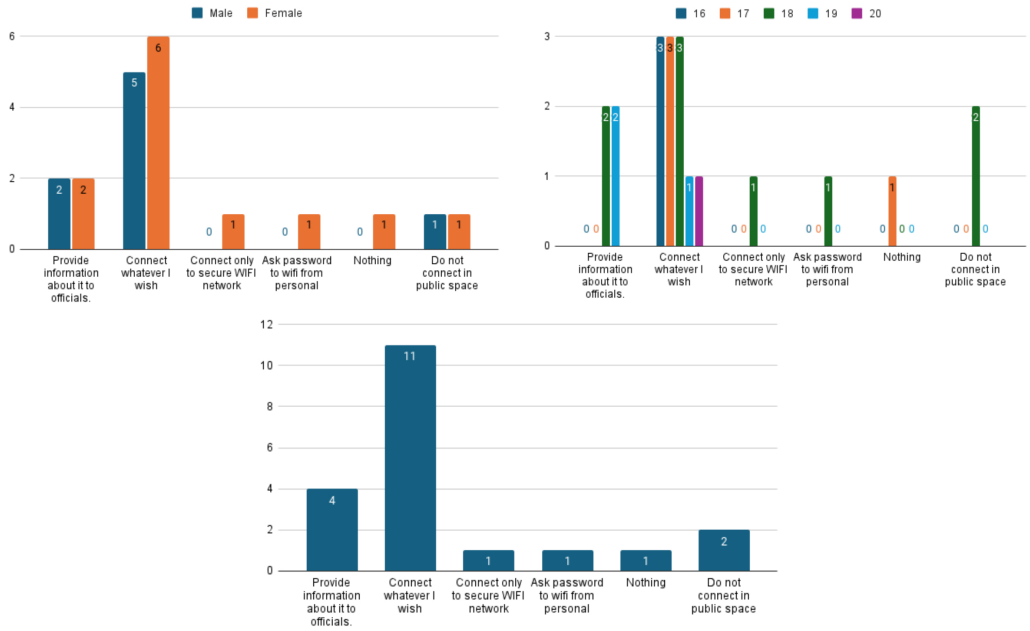

Figure 47. 29. You see two exactly the same WIFI on one spot. What do you do?

Questions from 30 - 32 (see Fig. 48-Fig. 50) check respondents skills to determine real email from malicious. By theory, if the user does not bite the message, it could be because of incorrect template usage, such as incorrect text size or design. By using the right template, there is more chance that the user will take a bite. In question 30 (see Fig. 48), most respondents chose the wrong email, which shows that respondents need to develop skills in understanding emails. According to results from question 31 (see Fig. 49), most respondents were right that the email in the picture was not real. Still, in question 32 (see Fig. 50), respondents were wrong about the second email. Also, the results of questions 31 (see Fig. 49) and 32 (see Fig. 50) show recursion in answers, which could bring the theory that if respondents understand that the first email was fake, the second one would make them less cautious and more vulnerable to attack. Such recursion could be seen in age 18 with female respondents and overall results.

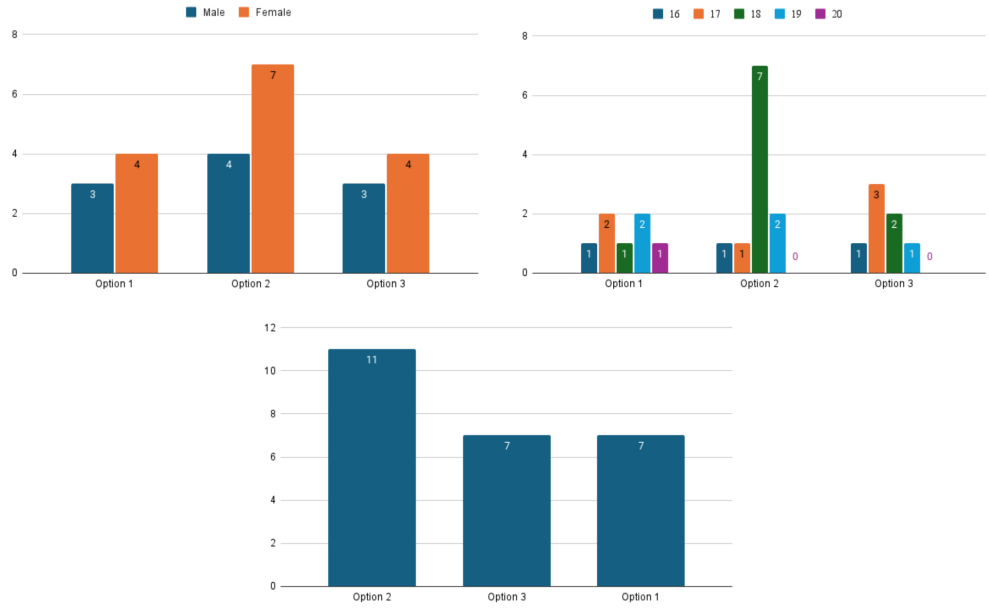

Figure 48. 30. Which one is the real email?

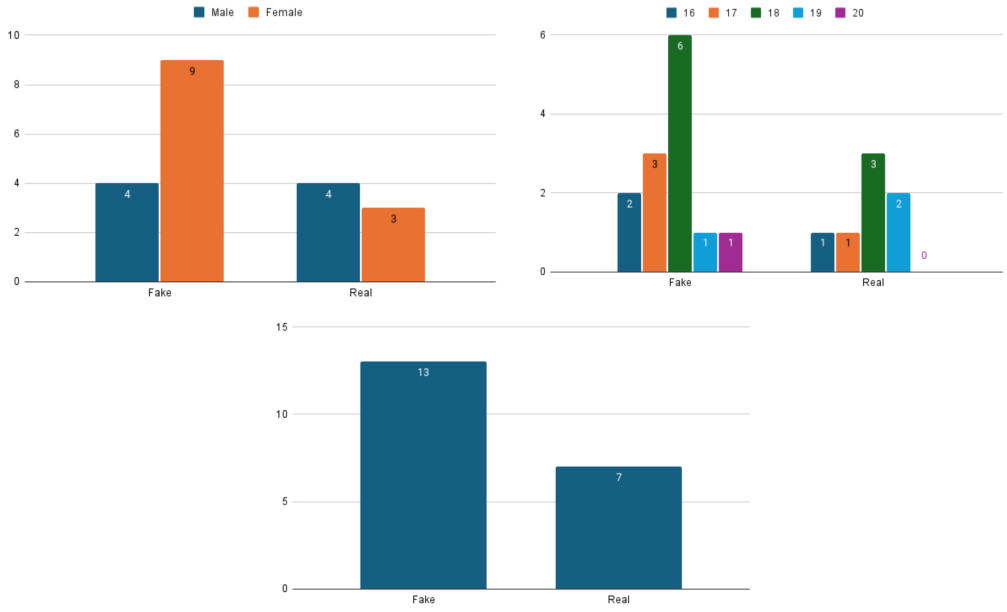

Figure 49. 31. Is this a real email or fake?

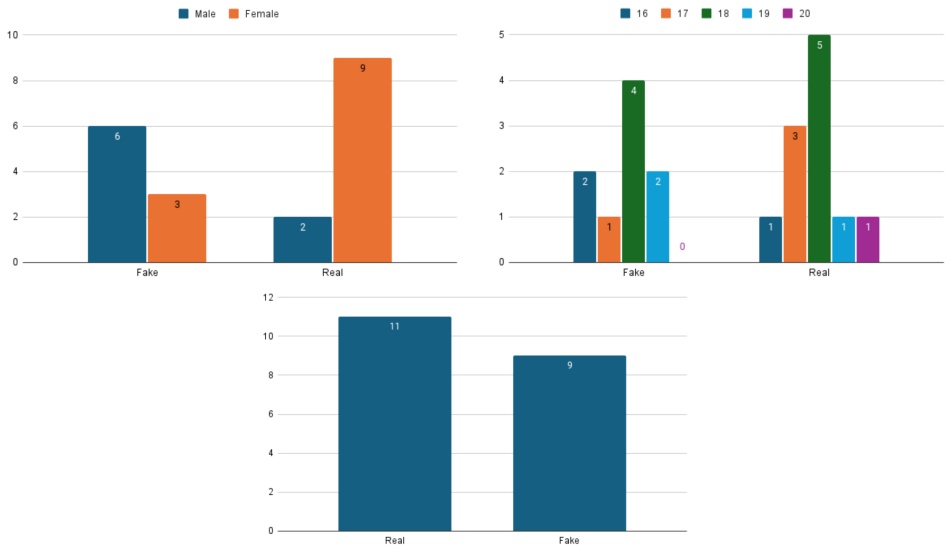

Figure 50. 32. Is this a real email or fake?

The last questions, 33-34 (see Fig. 51- Fig. 52), related to Deepfakes. Results show that subjects could be manipulated by using Deepfake as a tool for social engineering. In question 33 (see Fig. 51), most subjects chose a fake picture, but in question 34 (see Fig. 52), most subjects understood that the picture was fake. A hypothesis could be that for question 33 (see Fig. 51) was used a picture of a person who is not popular on social media. Still, question 34 (see Fig. 52) used a picture of a person known by a group of subjects. Because this group knows this person, it is simple to understand the structure of the person's body or face to confirm it.

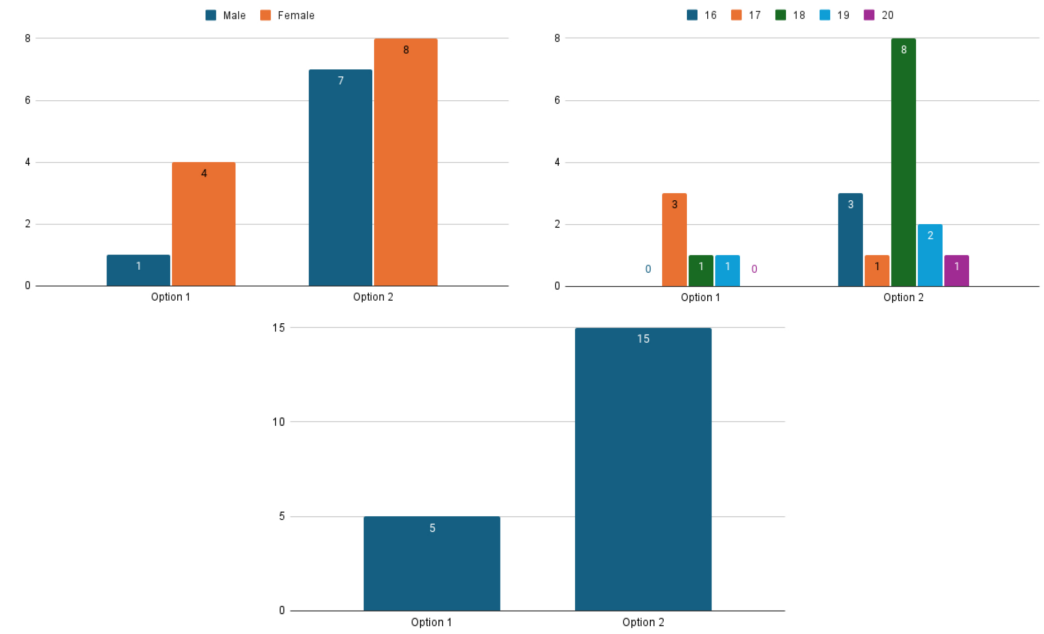

Figure 51. 33. Which one is real?

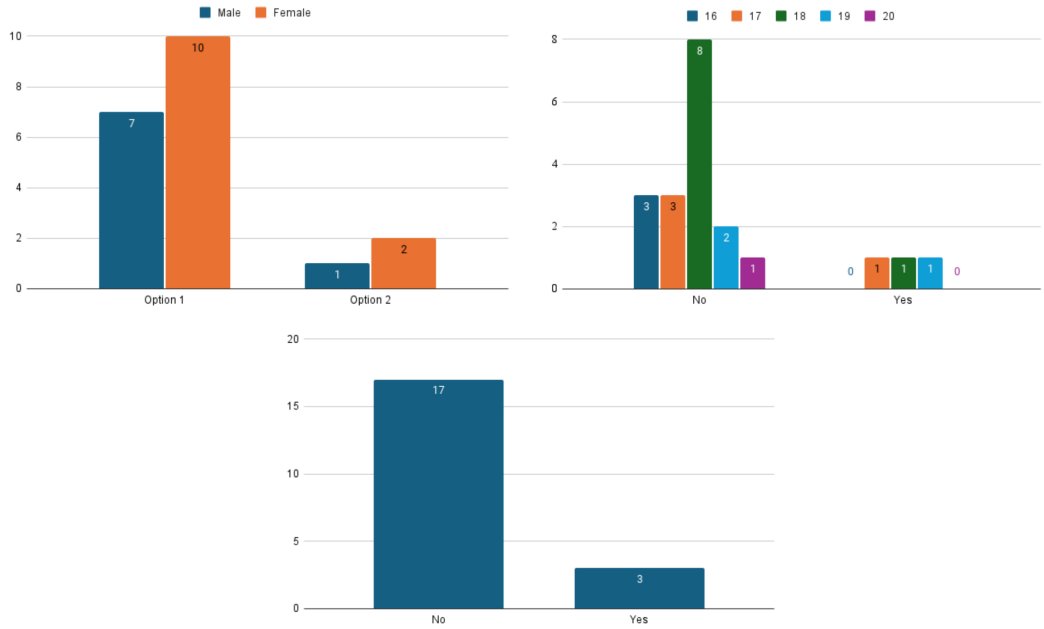

Figure 52. 34. Is it a real picture?

4.4 Key takeaways

The key points that could be highlighted are:

(i) **Respondents have very little understanding about social engineering and topic**. From question 8 (see Fig. 26), it is clear that respondents only know about popular topics in their surroundings that were discussed a few years ago. Because of that, they better understand what they are dealing with and can mitigate it. But if they deal with a topic about which they do not know, then there could be problems, such as Email Phishing or Pop-up windows, also from here comes another problem.

(ii) **Because of lack of knowledge, respondents are more vulnerable to techniques using technical aspects**. For example, in the Pharming technique from question 15 (see Fig. 33), an attacker could create a clone of a website that could be provided as legitimate. If the user ignores details on a website, he could send his personal data to the attacker.

(iii) **Respondents are vulnerable to free things**. This statement supports answers to question 29 (see Fig. 47), where free access to WIFI hotspots was given, and from question 28 (see Fig. 46), about the prize message in the Pop-up. Users need to understand that free things are also used for manipulation and could lead to losing personal information.

(iv) **Respondents react to social engineering when they lose something valuable to them**. Valuable objects could have different forms based on their form and use for holders. In social engineering, it could be, for example, their data. When a person understands that data which he is in danger, then he starts to think about how to deal with such a situation. Such theory could be proven by questions 30-32 (see Fig. 48 - Fig. 50), 17-19 (see Fig. 35 - Fig. 37). Because of that, training needs to include such methodology, which creates a trigger in the human mind danger of losing something important to him.

(v) **Differences between genders in understanding social engineering threats exist, but the differences are minor**. Data from the questionnaire shows no significant differences between women and men in answering questions. Still, some differences could be highlighted. Questions that could be highlighted are questions 11 (see Fig. 29), 13 (see Fig. 31), and 28 (see Fig. 46). In question 11, unlike men, most women do not change their password at some time. In question 13, most women delete email messages if they find something suspicious about the file in there; instead, men check it for malware. In question 28, Pop-up messages are clicked more recently by men than women.

(vi) **The age factor in detecting social engineering threats exists, but there are minor differences.**. By data, there was no significant difference in knowledge and skills about social engineering threats. Still, a small correlation exists in answers to questions that could be highlighted. Questions which could be highlighted are questions 13 (see Fig. 31), 25 (see Fig. 43), 28 (see Fig. 46), and 31 - 34 (see Fig. 49 - Fig. 52). In question 13 16, 17, and 19-year-olds open suspicious files in emails that they receive. In question 25, most 17-year-old school students think that happens bug when they revive a message from a friend who does not send it. In question 28, most 16 and 17-year-old school students click on a Pop-up message from the internet to receive their free prize. In

questions 31 - 34, primarily 17-year-old respondents provided the correct answers to questions related to understanding whether the email message and photo of a person was real or fake.

4.5 Summary

This section described the results of the questionnaire about social engineering knowledge and skills done by high school students. The provided data showed that high school students need to learn more about not popular social engineering techniques such as Smishing, Dumpster diving, Pretexting, etc. Also, they need more practical skills as examples of such techniques as Pharming, Email Phishing, etc. A more detailed review of each social engineering technique can be found in section 4. This data answers the research question SRQ1. Also, this data would be used for training creation in section 5. Due to a lack of time for development, the most relevant techniques would be used in training. They are described in Section 5.

Two theories were found during the data analysis. The first theory is that injection would be more successful if give something for free to the respondent. The second theory is that injection could have a lower rate if something valuable could be lost for the respondents in the injection process.

5 Gamification-based Training

This section describes a gamification-based training creation process, which includes game scenario writing, a description of tools and methods used in the development process, and the step-by-step development of the game. Also, it provides an answer to the SRQ2 question from Section 1.2 as a proof of concept of a one-platform solution for social engineering education.

5.1 Training program

The training program relates to education on different social engineering attacks and how to mitigate them in a gaming format. Because this research has a limited amount of time, we use in training social engineering attacks with which students from the first questionnaire have problem. Topics that would be used in training:

- **Basic knowledge about social engineering topics** - as was said earlier in the questionnaire in question 8 (see Fig. 26), it was found that 10-12 class respondents mostly know about Deepfakes, but in other areas, they lack knowledge 4. Knowledge about currently known social engineering attacks and how they work help mitigate future attacks if they have similarities with presently known ones.
- **Email phishing** - By results on questions 30 - 33 (see Fig. 48 - Fig. 51), it is clear that subjects have difficulties understanding whether an email is phishing or not, even with a hint in question 30.
- **Pharming** - According to the questionnaire results in question 15 (see Fig. 33), 13 respondents, in most cases, will change their credentials on the same page if they need clarification about whether their credentials are correct. This result could come from a need for more knowledge and practice about the Pharming technique; an indication of that idea could be found in the results of question 8.
- **WiPhishing** - By the results of question 29 (see Fig. 47), nearly half of respondents would connect to public WIFI if it is open.

Training is provided in a computer game format to educate the person on mitigating specific attacks chosen for this thesis. Before game creation, need to select the core gameplay of the game. For that, ideas were created for the game core, which gives a narrow view of the central gameplay core of the game.

- The game consist of various mini-games related to different topics. User can select specific topics from the main menu and play mini-games that teach him about the defined topics. Each mini-game is divided into two parts: an educational section

where user receive information about the attack and how it works and a simulation section where user engage in a game that mimics the real experience of an attack, helping them develop a mindset for future attack mitigation. After finishing a game, user can provide feedback to indicate their satisfaction, and the menu offers options to submit ideas for new games or topics and provide contact information for further involvement. User receive rewards and unlock higher difficulty levels as they progress.

- The game simulates a real-time work environment where user perform specific tasks using a workstation. During the game, user encounter events related to social engineering threats that can cause problems for themselves, their organization, or people connected to them. If user make too many mistakes, the game ends with consequences linked to the specific person or entity harmed by his actions. User earn achievements for various actions in the game, which come in three difficulty levels. The easy level has fewer mistakes and includes a mascot to help user understand their errors.

The second option, the real-time work simulation, was selected for game creation. This approach is intended to simulate real attacks, providing an authentic experience that helps user develop the right mindset for dealing with social engineering threats.

5.2 Game creation

This section provide the materials and the step-by-step game creation process. Game files can be found in the GitHub repository[4] or downloaded from Itch Io[5]. We also prepared a demo video of the project, which can be found on GitHub[6] or YouTube[7].

5.2.1 Game description

First of all, we need to describe in detail the steps of the game creation. Let's remember the game description from section 5.1; it simulates real-time work in the organization; each time, the user needs to work on specific tasks using your workstation. Sometimes, events happen between work, which is related to social engineering threats. This threat could cause problems for himself, his organization, or people related to him. If the user makes too many mistakes, then the game ends with an ending associated with a specific person to whom he caused harm. This game provides achievements for different actions and has three difficulty levels. Easy difficulty has less cause for the mistake, and the

[4] https://github.com/santeri13/SEEG
[5] https://blacktime05.itch.io/seeg
[6] https://github.com/santeri13/SEEG/tree/main
[7] https://youtu.be/eMPNReYooIE

mascot would help the person understand where he was wrong. When the user deals with social engineering, it is shown in the catalog, and he can read more about it. The scheme of the game is in Table 53 on page 68.

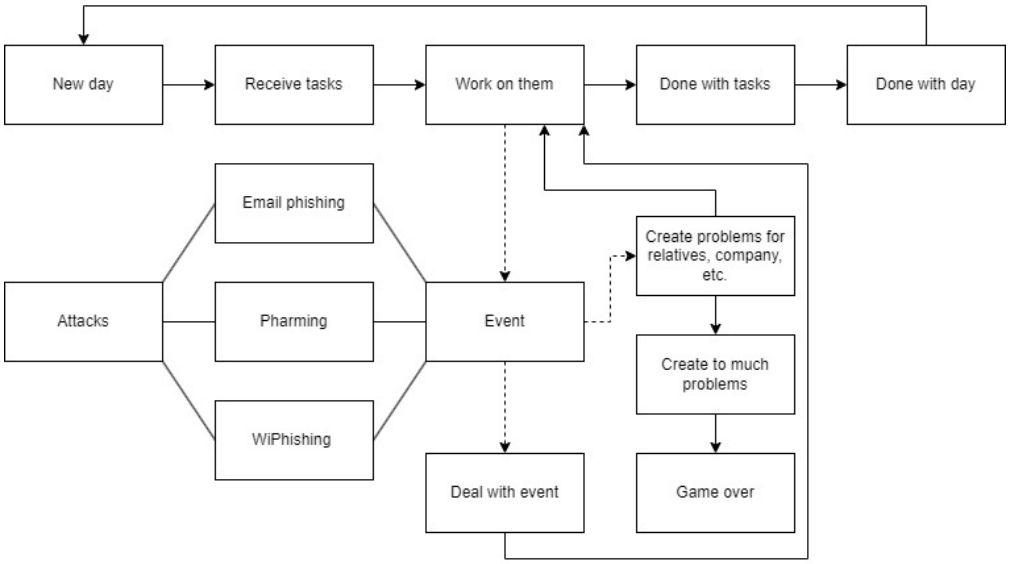

Figure 53. Game core description

Next, we need to identify the game genre and mechanics. In this process, need to remember that gamification elements need to be chosen from the game perspective and the Octalysis framework perspective. The game has a "Simulation" genre because of the imitation of work experience and social engineering threats and a "Role-playing" genre because of the role of another person in the organization.

When analyzing which mechanics must be taken to the game, here is a vital role in the Octalysis framework. The Octalysis framework is split into different parts to identify a better user experience from a human-centric approach perspective. The critical mechanics on which the game is based are "Theme and story" and "Visibility of progress" 2.4.3. When a person plays a game whose primary function is to teach something to the person, he needs to learn new things that he does not know. For that, we need to provide the experience as closely as possible, and for that, we need to create a story in which the user would feel comfortable and could impersonate himself in the character's situation. This gives him experience, which could be used further when a user is in a similar situation to what was in the game. Also, the person needs to understand that he learns something new in this process by some indication, which gives him an idea about this. Levels that show the same social engineering attacks are one of the solutions for this task. This helps the user to repeat early learned material. From another perspective, the user uses early learning of the material to find new ideas about the attack. This

would give him the idea that he understood the material shown earlier but, at the same time, learned something new. As optional for mechanics could be "Challenge" and "The opportunity of mastery" 2.4.3. The game provides a challenge for people who have yet to have a good amount of experience with social engineering attacks. Still, in the first place, its purpose is to teach people about mitigating social engineering techniques. The same could be said about the "Opportunity of mastery" mechanic 2.4.3.

5.2.2 Analysis of game through framework

The Octalysis framework consists of 8 parts such as (i) Epic Meaning and Calling, (ii) Development and Accomplishment, (iii) Empowerment of Creativity and Feedback, (iv) Ownership and Possession, (v) Social Influence and Relatedness, (vi) Scarcity and Impatience, (vii) Unpredictability and Curiosity, and (viii) Loss and Avoidance [23]. To understand how much the created game is human-centered, need to define different details based on the parts that the Octalysis framework has. The graphic, which describes various parts of the game from the Octalysis framework perspective, can be found in a graph 54 on page 71. The next part describes each element of the Octalysis framework included in their core drives, which describe the game idea from the human-centric side.

Epic Meaning and Calling motivate the player to action if he thinks that his action would make something on a grand scale. For example, if a person helps in research to create medicine for dangerous diseases. Using the same logic for the game could provide experience working with tasks close to companies in the same position. Such games help teach people how to mitigate such attacks and provide awareness about problems caused by a lack of knowledge of social engineering. If the game successfully offers new information to the player, he could help promote the game to his colleagues and friends. Also, as a first user, he would be interested in being connected to the project if it would solve a problem with a lack of knowledge about social engineering attacks.

Development and accomplishment are primary drives that describe a person's motivation to learn new skills and receive more profound knowledge about a specific area in which he is interested now or in a particular period. This also means that for better emotional and narrowed push, one needs to challenge the person so that the knowledge he receives would be more valuable for him. This game provides both difficulty and something new to the user, which he could be interested in, and this is skill and knowledge about social engineering. Empowerment of Creativity and Feedback drive a person's ability to create something in or for the product. Humans are creative creatures, so they try to create something new if they have an idea and a desire. The same goes for games in which they are interested. If the game has elements that allow the person to be creative, then he would use this chance. Because this game is a new product, a person could be interested in helping with content, which would be added in the future by sending reviews with ideas about new content. For example, new ideas for levels that describe live situations with social engineering attacks.

Ownership motivates a person to receive something new for himself, which he could acquire and transfer. There could be similarities between Development and Accomplishment, but the difference is their goal. In Development, a person is motivated to learn something new by passing challenges. Instead, ownership drives the person to only receive an item with which he would have a connection with the game. In this game, the user would receive knowledge about different social engineering attacks, which he, as the user, owns and could transfer to other people or recommend the game as learning material. Also, the game would have achievements that a person owns by passing levels and passing them on the conditions specified in the accomplishment.

Social influence motivates people to play games because of the impact of something or someone. For example, when someone recommends a specific game because of exciting gameplay, challenge, etc. Another example is when games have strong marketing campaigns that drive people to play them. An example of such a tactic could be Cyberpunk 2077, which shows good graphics and exciting gameplay in trailers, has merch based on this game, etc. In situations where educational games could be used as learning material, people use them because they like to receive knowledge about social engineering. If they like it, then by giving suggestions from person to person to play this game, other people would be a social influence to play this game.

Scarcity and impatience drive the person because he likes to reclaim something rare. It could be an achievement, an object, or made by the community or in a game challenge. This game provides a challenge for user to go through until the game ends, knowledge of which person will receive, and rare achievements. Unpredictability and Curiosity play a role in a person's motivation for new things. It drives a person to receive new experiences and knowledge about something that he finds rare or for the first time. Games that teach a user something new could be found rare, and games that teach social engineering are rare. This motivates a user to try interesting concepts by passing real threats and learning something new about a topic he knows little about. Loss and Avoidance drive a person to avoid negative situations. An example could be taken from a rating table in MMO where a user tries to avoid losing his rank. In a situation with the game for the thesis, a person would be driven by the idea that he could lose something personally, such as money or critical information because he did not pass this game.

Figure 54. Octalysis game framework

5.2.3 Game development tools

Game development is a complex process that requires tools for creating scenarios, frontend mockups, a game engine for the game backend, etc. Different games need different tools based on preferences, goals, and game genres. For this game, the tools required for development are: (i) **Game engine**, every game requires an engine on which this game code would be built. (ii) **Application mockup**, before writing a code, need to figure out how the game would look and how it would be played from the view of a game designer. This makes the development process of writing code easier and helps make changes and integration faster. (iii) **Scenario writing application**, because one of the game's main elements is the story, it is vital that it is logical and creates the right

mindset for people who play it.

First, let us discuss the game engine. The criteria for choosing a specific engine are as follows: (i) It has tools for game development in a 2D environment and is simple to use. Because the author is not a professional game developer, it would be better if the engine had simple instruments for game development; (ii) the engine already has a successful project that could describe how the game development process goes. This also gives the author learning material by which he could learn new things about engine faster. (iii) The engine is still maintainable. Famous examples could be provided 3 options:

(i) *Unity* is one of the most popular and widely used game engines, known for its versatility and cross-platform capabilities. It is favoured for both 2D and 3D game development. Unity is renowned for its popularity, extensive community support, and robust cross-platform capabilities, making it a good choice for various projects. The vast Asset Store and user-friendly interface enhance its appeal, especially for beginners. However, it faces challenges with performance optimization for high-end graphics, complexity in managing advanced features, and, most notably, a controversial pricing model introduced in 2023 that includes a runtime fee based on game installs, causing significant backlash from the developer community.

(ii) *Unreal Engine*, developed by Epic Games, is a powerful game engine known for its high-end graphics and comprehensive toolset. It is often used for AAA game development and complex simulations. Unreal Engine excels in high-end graphics, providing a comprehensive suite of animation, physics, and rendering tools. The Blueprint visual scripting system allows for rapid prototyping, and its strong community and marketplace offer extensive resources. However, Unreal Engine has a steeper learning curve. It is resource-intensive and challenging for smaller projects or less powerful hardware. It also employs a royalty-based pricing model, requiring developers to pay a percentage of revenue after surpassing a certain threshold.

(iii) *Godot* is an entirely free and open-source game engine known for its lightweight design and ease of use. It supports both 2D and 3D game development, focusing on simplicity and efficiency. Godot open-source nature allows for extensive customization without hidden costs, making it a cost-effective choice for developers. Its node-based architecture and flexible scripting options (supporting GDScript, C#, and VisualScript) simplify development and cater to beginners and experienced developers. However, Godot has a smaller community than Unity and Unreal, fewer available assets, and might not match the performance capabilities required for high-end AAA games.

In discussing which engine is better for developing a computer game for educational purposes, the choice narrows down to Unity and Godot. Unreal Engine primarily focuses on high-end 3D graphics, making it unsuitable for this project's first criteria. Between Unity and Godot, Godot emerges as the preferable option. Since 2023, Unity has faced significant criticism for its commercial decisions, notably introducing a runtime fee based on game installs. This new pricing model has caused considerable discontent among

developers and companies, leading many to explore alternative engines like Godot. Unity's future has become uncertain due to these controversial changes, prompting developers to seek more stable and developer-friendly alternatives.

Godot, with its open-source nature, eliminates the risk of unexpected costs and provides a transparent, cost-effective solution for game development. Its lightweight design and efficient performance make it particularly suitable for educational games, where high-end graphics are less critical. Godot node-based architecture and flexible scripting options simplify the development process, making it accessible to developers of all skill levels. In conclusion, while Unity and Unreal Engine have their strengths, Godot's cost-effectiveness, transparency, and developer-friendly features make it the optimal choice for creating educational games, especially in light of the recent instability in Unity pricing policies.

As for scenario application, the main criteria are as follows: (i) Have instruments for writing each part of the story. The story has different parts, such as the main storyline, side stories, level stories, etc. It is crucial that the application connects each one of them logically but also holds them in their story part. (ii) Have a simple interface and functionality. Because the author is not a professional story writer, it is essential that the interface is simple in use and has the functionality that helps to connect each part of the scenario into one logical story. Searching instruments that could go under such criteria, was found 2 options:

(i) *Nuclino* is a collaborative knowledge management tool designed for efficient information sharing. It integrates a wiki, task management, and knowledge base elements into a single platform. Nuclino strengths include its intuitive, user-friendly interface and real-time collaboration features, which facilitate effective teamwork and document sharing. The structure of the tools "nodes" and "collections" makes organizing and accessing information easy. At the same time, its cloud-based nature allows for access from multiple devices anytime, anywhere. Integration with other tools enhances its versatility and support for rich text editing, and various templates streamline content creation. However, Nuclino reliance on an internet connection can be a drawback, as it limits offline functionality. Additionally, while it excels in collaborative settings, it may not offer the depth of data structuring required for intricate or highly specialized information needs.

(ii) *Obsidian* is a powerful note-taking and knowledge management tool that emphasizes personal knowledge management through a network of linked notes. It is highly customizable and operates locally on your device. Obsidian strengths lie in its ability to create a rich, interlinked network of notes, making it ideal for managing complex information and personal knowledge bases. Its local storage ensures data privacy and offline access, and the extensive plugin ecosystem allows for a high degree of customization. The markdown-based format offers flexibility in note-taking and integration with other tools and formats. However, Obsidian learning curve can be steep, particularly for user

unfamiliar with markdown or advanced note-linking concepts. Additionally, its focus on personal use and local storage can limit collaborative features and integrations compared to cloud-based solutions.

Nuclino stands out as the preferred choice for writing game scenario. Unlike Obsidian, which offers a highly customizable but complex interface, Nuclino is designed with user-friendliness in mind. Its straightforward, intuitive interface makes it easy for user to quickly get up to speed, reducing the time needed for training and minimizing the learning curve. Nuclino real-time collaboration features and cloud-based access facilitate seamless teamwork, allowing users to work together effectively regardless of their location. The ability to easily create, organize, and share documents through a clear and straightforward interface ensures that user can focus on their work rather than struggling with the tool itself.

The last is the application for creating a mockup for the game. The main criteria for application are: (i)provide functionality for fronted creation; (ii)tools to show game workflow or how it would do scene by scene; (iii)easy to use for beginner game developer. Searching tools by the provided criterias found 3 options:

(i) *Figma* is a cloud-based design and prototyping tool known for its robust collaborative features and intuitive interface. It is widely used for UI/UX design. It offers a comprehensive suite of tools for creating interactive prototypes and design systems. Figma primary strengths include its real-time collaboration capabilities, which allow multiple users to work on the same project simultaneously, enhancing teamwork and feedback integration. The cloud-based nature of Figma ensures that designs are always up-to-date and accessible from any device. Its extensive design tools, including vector graphics, prototyping features, and component libraries, make it a powerful choice for complex design projects. However, Figma reliance on an internet connection can be a drawback, as it limits offline access. Additionally, while its broad functionality is advantageous, it can sometimes overwhelm user who need a more streamlined design approach.

(ii) *Moqups* is a web-based tool for wireframing, prototyping, and creating visual mockups. It focuses on simplicity and ease of use, making it suitable for quick design iterations and early-stage project planning. Moqups stands out for its simplicity and ease of use, which makes it an excellent choice for rapid prototyping and creating basic wireframes. Its drag-and-drop interface and pre-built templates streamline the design process, allowing user to quickly create and iterate on design concepts. Moqups also supports real-time collaboration and integrates with various tools for added functionality. However, Moqups may lack some advanced design and prototyping features in more specialized tools like Figma. Its functionality is more limited compared to Figma tools, which offer extensive design capabilities and customization options.

(iii) *Mockplus* is a design and prototyping tool emphasizing ease of use and efficiency. It provides a range of features for creating interactive prototypes, wireframes, and high-

fidelity designs. Mockplus offers a user-friendly interface and a comprehensive set of tools for wireframing and high-fidelity prototyping. Its drag-and-drop functionality and pre-designed components facilitate rapid design and prototyping. At the same time, its interactive features enable user to create realistic prototypes. Mockplus also supports real-time collaboration and integrates with other design tools for enhanced workflow efficiency. However, Mockplus may not offer the same advanced design capabilities and flexibility as Figma. Its interface, while simple, might not cater to more complex design needs or extensive customization requirements.

Figma is the ideal choice for game development due to its alignment with essential criteria. It offers robust functionality for frontend creation, allowing detailed design and interactive prototyping of game user interfaces and visual elements. The tool advanced prototyping features enable user to create interactive flowcharts and scene-by-scene walkthroughs, effectively showcasing game workflows and transitions. This makes it easier to visualize the game structure and user interactions. Additionally, Figma intuitive interface and extensive library of pre-built components make it highly accessible for beginner game developers. Its user-friendly design, real-time collaboration, and cloud-based access ensure that newcomers can quickly grasp and utilize its features without a steep learning curve. Overall, Figma comprehensive design capabilities, workflow visualization tools, and ease of use make it the superior choice for both creating detailed game elements and demonstrating game workflows.

5.2.4 Game scenarios

For a game oriented on creating a story that could teach a person something new and create the world around it, one needs a scenario. A written scenario helps engage the player in playing the game by working with mechanics which is written in a story or by the exciting story itself, adding narrative depth that shows the player his importance to the world through his actions and creates an emotional impact, which helps create a positive experience for the player and create an opportunity that he would replay the game. A well-crafted scenario immerses players in the game world, capturing their attention and keeping them engaged throughout their gaming experience. Engaging scenarios give players a sense of purpose and motivation to progress through the game. Scenarios contribute to the depth of the game's narrative, offering rich storytelling opportunities that can evoke emotions, provoke thought, and create memorable experiences. Players can explore intricate plots, complex characters, and dynamic relationships within the game world through scenarios. Well-executed scenarios can evoke a wide range of emotions in players, including joy, sadness, fear, and excitement. Through compelling storytelling and immersive gameplay, scenarios can create emotional connections between players and the game world, leaving a lasting impact long after the game is completed.

The game scenario is based on two factors: (i) this game requires social engineering topics, which were chosen by the results of the first questionnaire, and (ii) the game

scenario needs to be human-centered. As was said earlier, each aspect of the product somehow affects the user's experience in a human-centered way. Each scenario for visual or audio content affects the user emotionally or creates an idea in his mind. Because of that, the scenario must have elements of real situations to simulate social engineering attacks and build the scenario around users who do not know much about such kinds of attacks.

The story starts with a letter accepting a user to work in a big organization in the position of 2-level support. User will work from home on a simulated computer environment where are installed all needed tools. At the start of the game, user will learn how to work with given tools with the help of the organization mascot, Timmy and virtual cat assistant. He shows each tool the organization uses and provides information about the "book of knowledge," from which the user can read strict rules that organization employers should follow if they like to be safe from cyber threats and hold strong organization security. After the tutorial, the user has ten levels of the game, and each day, a cyber event could harm the user, organization, or relative if a user is not extra cautious. Below is a description of attacks used to create social engineering attacks for the game.

Attack scenarios related with WiPhishing:

(i)**VPN access** - The user received a work email that today, the organization where the player character works changed their VPN access point to another because of technical problems. Suppose the user changes the access point written in the message. In that case, the attacker gets access to information that flows in the user character network. The attacker receives access to the organization network and user character work credentials from this information. Then, the attacker changes records in the organization database, and by that, it makes an impression on the user. This creates an impression on the user that next time, he needs to be more careful about instructions from email. If the user reports this email, he receives a positive message about the right action that creates a positive impact on the user and that he understands how to mitigate such an attack.

Attack scenarios related with Pharming:

(i) **Email message link** - The user receives a work email message that every employee of the organization is required to log in to the new version of the record system and provide their personal and work information so that the technical team can connect their current data from other parts of the network to the system. The email includes a link that provides access to the new version of the record tool. If the user follows the link to the website and provides all the information, he receives information from the bank that someone tried to make a loan in his name.

(ii) **Path change to organization webpage** - The organization sends an email to all employees. Because of a recent cyberattack, they have problems accessing some organization webpages. A link for these pages is included with the email, which the organization asks to log in to check if all employees have access. When the user puts his credentials on this page, he receives a message that someone used his credentials to

retrieve essential data from the organization's server.

(iii) **Receive email message with prize link** - On work email, the user character receives an email that provides information that the user won a prize, which he could receive by going to the provided link. The user needs to provide his character's personal information to receive an award. When the user goes by this link, all information is already placed.

Attack scenarios related with Email phishing:

(i) **Email phishing with work email** - user receives a message with changed work email.

(ii) **Changes in mail template** - The user receives an email with a legitimate address, but the template is different from the standard.

(iii) **Send your personal data** - The user receives an email from one of the organization executives stating that they require the user's character personal data for double-checking in their system.

5.2.5 Game mock-up

The game mock-up includes a visualization of how the game works and the design of each element. As was said previously, all mock-ups were done in Figma[8]. Also, this mock-up does not represent the final game design and could have differences in design and mechanics. This section provides ideas used in the mock-up but not included in the final game release or ideas that were changed in the development process.

First, the game included ten levels, representing ten in-game days. It comes from the idea that a workday does not always have a social engineering attack. It was done to teach people to separate accurate information from information that is used for social engineering attacks and to learn how to differentiate real information from fake information. This idea was not included in the game because, in the process of writing scenarios, decision were made to provide three attack examples on each technique. If we include the levels plan and the final level, which contains all social engineering techniques attacks, then the maximum amount of levels is already 10. Because the game was planned small and short for better immersion, it was decided to include only levels with social engineering techniques.

Also, from the planned mock-up, money was removed to indicate a mistake between the user and different relatives' dialogue. It was changed on simple mistake indication. It was done to simplify the user's understanding that he made a mistake on a specific level. Relatives were removed because the idea was too ambitious for this game in a short development period. As was said earlier, the author is not a professional game developer and game designer, and ambitious ideas that he could not implement in a given

[8] https://www.figma.com/design/wet7uFZvKED7ZQNkdrgElF/Game?t=188QUWU6tsp9snG4-1

time frame could come in the process of planning. Still, it is also essential to understand that sometimes it is better to remove the concept than take more time to implement it.

5.2.6 Game code examples

Game logic is divided into Instruments, Levels, and Menus. The instruments category contains code for in-game tools that players use. In most cases, they are used to show something to the user and send a signal when the user does an action related to a specific tool. For example, figure 55 shows part of the code related to the Book module, a tool by which players can read in-game organization rules. It does not provide complete code; it only provides part of it. The full code can be found on GitHub[9].

[9] https://github.com/santeri13/SEEG

```
extends Control

signal CloseBook

func _on_vpn_pressed():
  $Tablet/TextureRect/VPN_note.show()
  $Tablet/TextureRect/VPN_note/VPN_note_name.text=tr("VPN")
  $Tablet/TextureRect/VPN_note/VPN_note_text.text=tr("VPN is used to
      receive access to our organization's network. As second-level
      support, you are forbidden to change any settings in the VPN
      connection. If required, we will send you a private email
      message where we will write about the day and time when you need
       to provide your device to the service center.")


func _on_close_vpn_pressed():
  $Tablet/TextureRect/VPN_note.hide()


func _on_close_report_pressed():
  $Tablet/TextureRect/Report_note.hide()


func _on_reports_pressed():
  $Tablet/TextureRect/Report_note.show()
  $Tablet/TextureRect/Report_note/Report_note_name.text=tr("Reports")
  $Tablet/TextureRect/Report_note/Report_note_text.text=tr("Each
      organization worker must be cautious in their actions, which
      could harm the organization. If you find something suspicious,
      send a report about it, but please double-check if you are sure
      that something you found is dangerous.")
```

Figure 55. Instrument example.

Levels contain the logic of each day, such as which social engineering attacks to use, which email messages are received by the player, and how tools would work based on which day the player is right now. Figure 56 shows an example of code for the first level. It does not provide complete code; it only provides part of it. The complete code can be found on GitHub[10].

[10] https://github.com/santeri13/SEEG

```
extends Control

signal pressedEnter

var languages:Array[String] = ["en","ru","et"]

func _ready():
  load_data()
  change_language(languages[language])
    $GameStart/Wallpaper/List_of_tasks/Text_List_of_task.text="Task:\
       nOpen Email"
  var emails = []
  emails.append("support_admin@utcorp.com,Today tasks,Today's task
     involves updating the tracking code ZP9538. Change the arrival
     destination from Spain to Helsinki and the arrival date to
     21.05.2024. Also there's a modification required for GV4210.
     Update the departure date to 17.01.2024.,OK,'")
  emails.append("tech_guy@utcorpi.com,VPN access change,Can you
     change your VPN path to 101.0.0.0/24. This is a new path for new
      tools; our team needs to check if it works properly.,malisiouse
     ,'")
  var file = FileAccess.open("res://Backend/Text Files/Email/inbox.
     txt", FileAccess.WRITE)
  for email in emails:
    file.store_line(email)
  file.close()
  $GameStart/Wallpaper/Vpn.connect("hacked",_hacked_message)
  $GameStart/Wallpaper/Email.connect("RightReport",_correct_report)

    func change_language(lang:String) -> void:
  TranslationServer.set_locale(lang)
```

Figure 56. Level example.

The menus category contains code for different menus, such as the main menu, where the user could start the game or change language. Figure 57 shows an example of code from the Menus category for the menu, which shows additional information about social engineering attacks. It does not provide complete code; it only provides part of it. The complete code can be found on GitHub[11].

[11] https://github.com/santeri13/SEEG

```
extends Control

var save_path = "user://data.save"

var languages:Array[String] = ["en","ru","et"]

func _ready():
  load_data()
  change_language(languages[language])

func save():
  var file = FileAccess.open(save_path, FileAccess.WRITE)
  file.store_var(level)
  file.store_var(mistakes)
  file.store_var(money)
  file.store_var(VPN)
  file.store_var(Wrong_path)
  file.store_var(Wrong_path)
  file.store_var(Maliciouse_link)
  file.store_var(Data_protection)
  file.store_var(Maiciouse_email)
  file.store_var(Maiciouse_email2)
  file.store_var(language)
```

Figure 57. Menus example.

5.2.7 Game testing

The purpose of testing is to see how the frontend elements of the game are friendly for the target user and how the backed features work correctly. If go by details of frontend testing, then: how aspects of UI show correctly on the user monitor because the first idea was to scale elements of UI to user monitor size, how comfortable is a user with ingame instruments which game provides from design and user interaction perspective, if user understand instructions which game offer and if in game are not grammar mistakes. From the backend side: find bugs related to in-game instruments work, that the game saves player progress so that he could start the game from the place where he stopped and that all examples in the encyclopedia open when they are found in the game if the levels work correctly based on player's reaction. The game was tested manually by two people from the same target group who were not participating in the research. It was done that later when the author began to test this game on real subjects, they did not know what would be in the game, which helped to provide more precise data.

For testing purposes, different models were analyzed to understand which is more comfortable for this game development in the current stage. For that, the author chose Waterfall, V-Model, and Agile models. The Waterfall Model (refer to Fig. 58) is a

traditional linear approach to software development, where the entire process is divided into distinct phases, each with specific goals and deliverables. The output of one phase serves as the input for the next, creating a sequential flow from requirements gathering to final deployment and maintenance. This model's advantages are a structured and organized approach from the start of development, a definition of early requirements not to change them in the development process, and a well-documented process to define what will need to be tested in the product. The disadvantage could be that this model has only a one-way approach. So, if the development build was changed, all processes must start again.

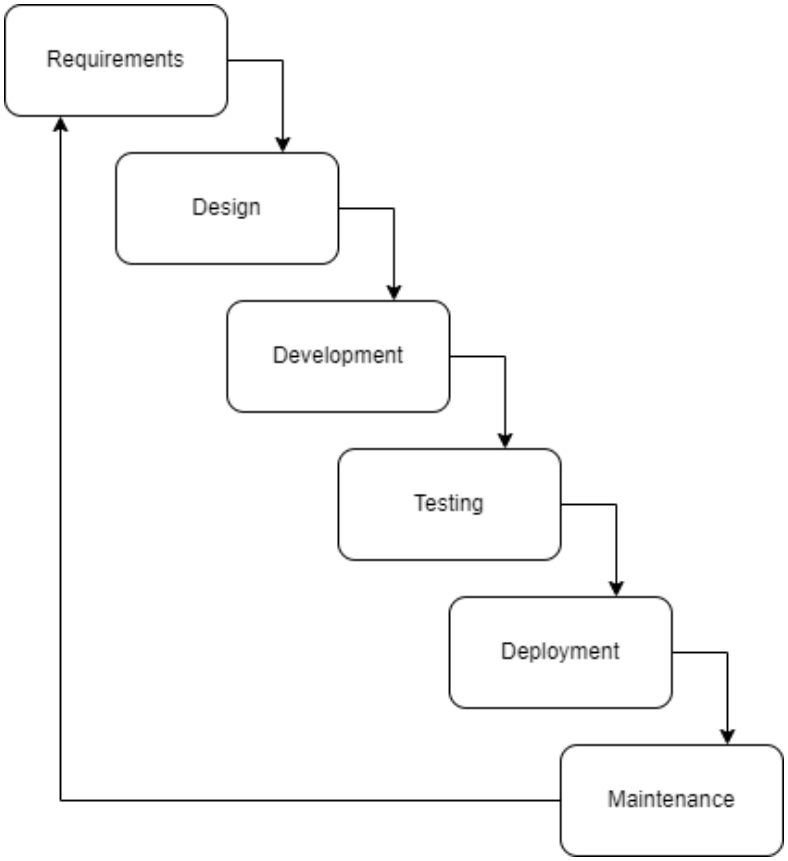

Figure 58. Waterfall model

The next one is the V-model. The V-Model is a software development methodology that combines the strengths of the Waterfall and Agile models. Like the Waterfall Model, it follows a structured, phased approach but introduces greater flexibility by testing activities throughout development. This creates a V-shaped pattern, where the development phases (planning, design, coding) align with corresponding testing phases

(unit testing, integration testing, system testing, acceptance testing). An example could be found in table 59 on page 83. As an advantage, this model has a phase of testing that checks how requirements chosen for the product are possibly integrated into the product before product development. This provides a comprehensive product analysis before the development phase and gives an overview of features that could be changed. As a disadvantage, this model requires detailed documentation about each aspect of the product and good coordination between different teams that write requirements for the product.

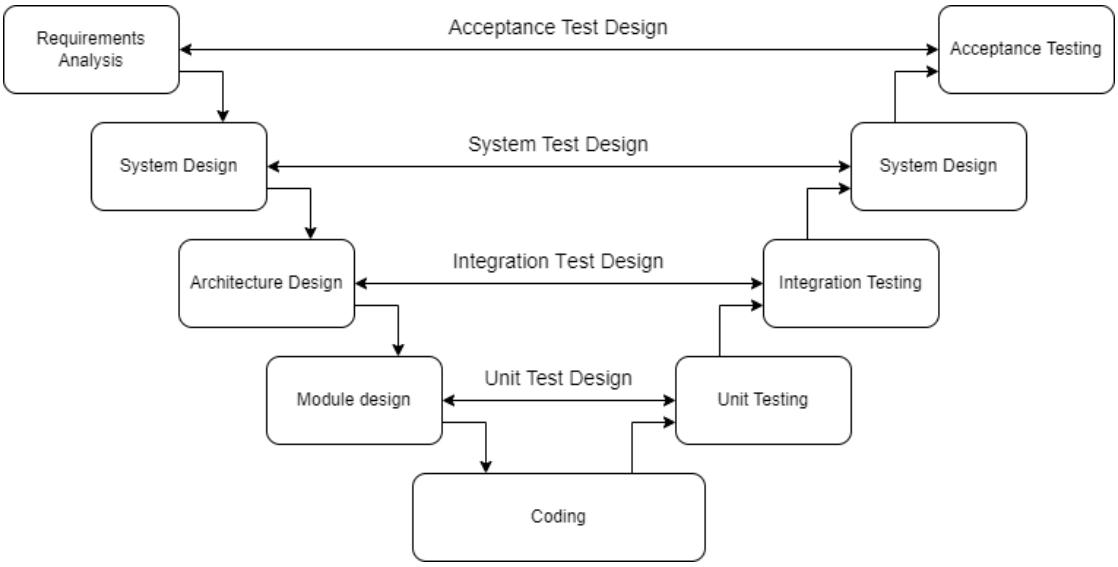

Figure 59. V-Model

The last one is the Agile model. Agile testing is a practice that follows the rules and principles of agile software development. Unlike the Waterfall method, Agile testing can begin at the start of the project with continuous integration between development and testing. Agile testing methodology is not sequential but continuous. An example of this model can be found in table 60 on page 84. This model provides =fast changes because tasks are split into smaller ones, with fewer test case writing requirements. However, because of that, the agile testing model does not provide much information about testing quality. By identifying the advantages and disadvantages of different models, the decision was made to use the Agile model. This game is not a big product that requires significant documentation. Also, the testing model was chosen after the end of the game development, so the V-model cannot support this game testing. Waterfall is ineffective because if something happens, then the project needs to start again from the start, which requires a lot of time, which this research does not have.

Changes for games were made during the development process, so each time testers

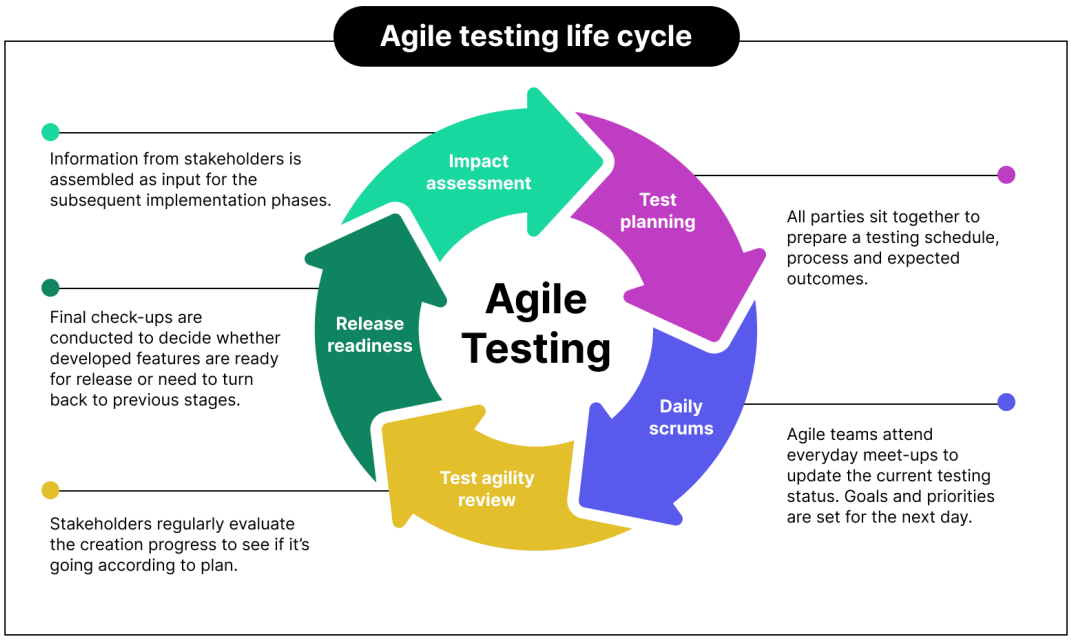

Figure 60. V-Model [24]

found a new bug, they provided logs about it, and the game was updated as soon as possible. Based on the testing results, it was found that some UI elements scale incorrectly when the user changes the game's screen size, so it was decided to make the game screen size 1280x720. Also, testers were uncomfortable with the fact that they did not see how many mistakes they made. For that, a mistakes counter was added, which showed how many mistakes the user had made by game time. From the testers' words, they were too bored to start the game again if they received five mistakes. For that, mistakes counter until game over stays as it is, but mistakes go to 0 if the user receives game over. That way, user could start the game from the last level and receive a more pleasant experience. It still provides an element that user can lose in the game process but provides a more pleasant experience. Also, in such a way, the user could repeat the activity on the level if he failed it last time, which gives him additional training. The instruction screen was moved under the ingame monitor so that the user better see the instructions text. Also, grammar mistakes in text were cleared on different levels. Many bugs related to in-game instruments and save files were found from the backend side, which also affected the encyclopedia opened examples. For example, there was a problem with one domain for phishing a website example. Because some elements of the scenario were changed in the game development process, some text parts were changed and were not integrated into

the game. Also, there were problems with the final level because some functions were not integrated at this level.

5.2.8 Game prototype

This section shows and describes the prototype of the game used in training. First, the thesis provided a general description of the game, followed by each essential element and how this game teaches players about social engineering.

The game has eight levels, each representing one example of a social engineering technique and one level with examples from each. Also, the game has a tutorial level that describes to the player how he would use in-game instruments and his mission. Going through the game, the player would open examples in the Encyclopedia, which represent different social engineering techniques and how to mitigate them. The game is translated into Russian, Estonian, and English.

The game starts from the main menu where the user starts the game, see Encyclopedia examples, or exit the game (see Fig. 61). Also, in the menu, the player could change the language. Compared with other projects that do not provide information on different languages, that could close the game for specific people who do not know a particular language [36, 34]. Also, social engineering concentrates on communication with specific individuals, and language plays a massive role in this. Because of that, it is better if players use suitable language for themself. The same goes for training experience and remembering specific information. Because this game was provided for people who live in Estonia, it includes the 3 most used languages: Estonian, Russian, and English.

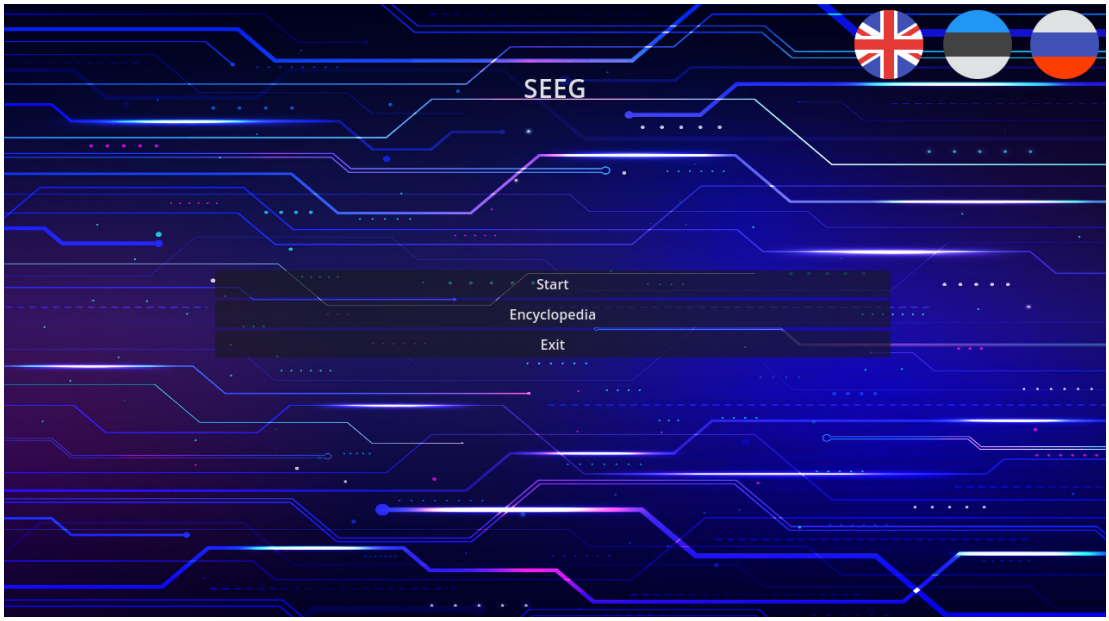

Figure 61. Game main menu

Next is the encyclopedia (see Fig. 62). As said earlier, players could read about examples of chosen social engineering attacks. When the user opens this game for the first time, examples are closed for the user. Each time a player passes a specific level related to the social engineering attack example, they will open. Other projects only provide training that creates reactions to particular techniques and gives little information [36, 34]. Still, sometimes, a person must explain this and how it works. This game gives people training and information on particular attacks and explanations.

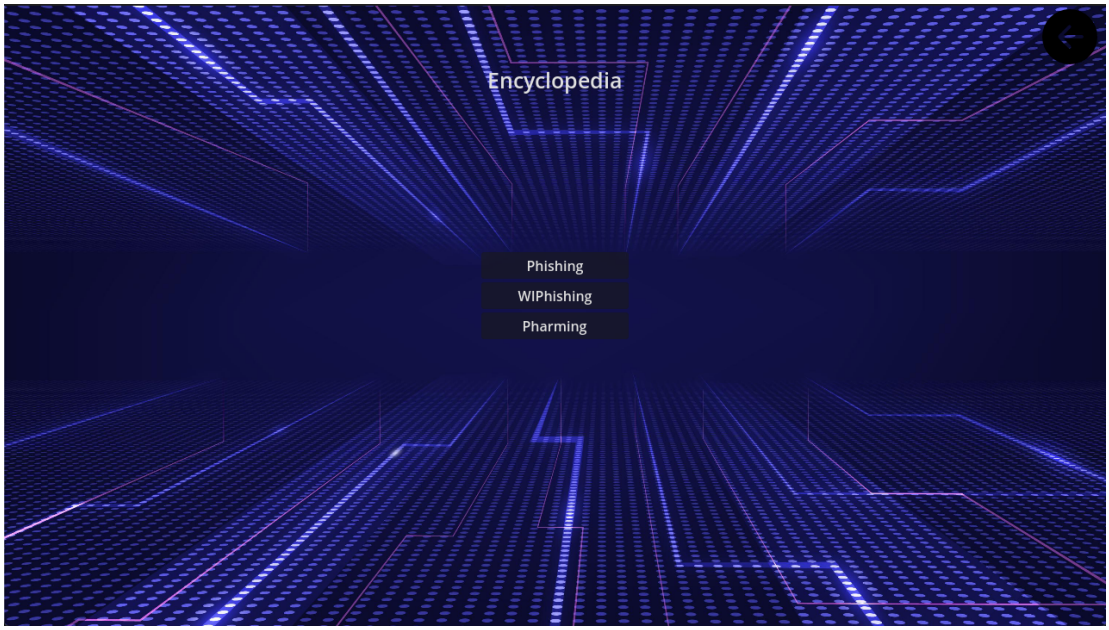

Figure 62. Game Encyclopedia

When the player clicks on the button start in the game menu, he goes through a tutorial describing the background of his character, his tasks, and the in-game instruments he would use. The player starts working in a organization named "CORP" as second-level support. His main task is to change cargo delivery records if required. The player could use instruments such as email for receiving tasks and answering emails (see Fig. 63), applications for changing VPN access points (see Fig. 65), applications for changing information in records (see Fig. 66), and web browsers (see Fig. 64). This game provides training that simulates the situations where users could deal with specific social engineering attacks. Because of that, a person better understand the exact situation in which he could be with the particular attack. He could apply this knowledge and skills to other situations with actual attacks.

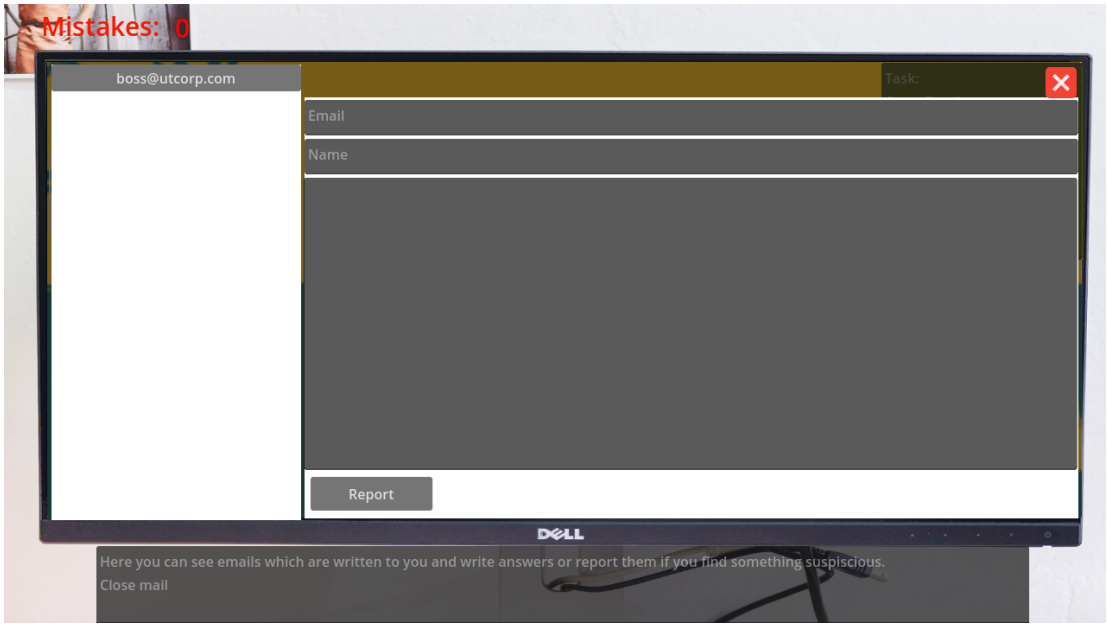

Figure 63. Game email application

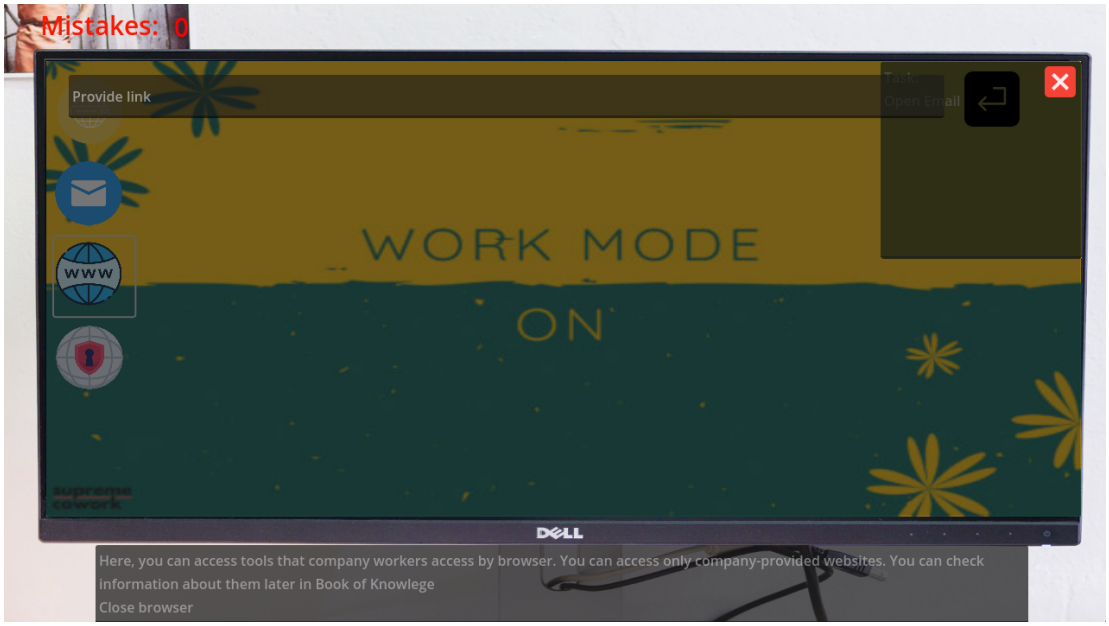

Figure 64. Game web browser

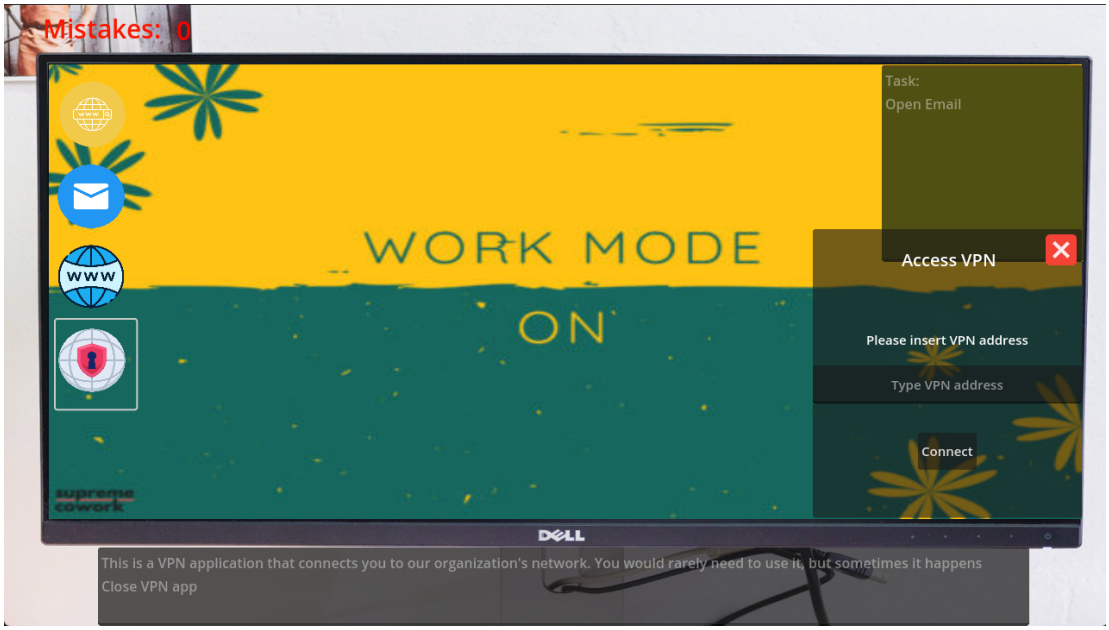

Figure 65. Game VPN application

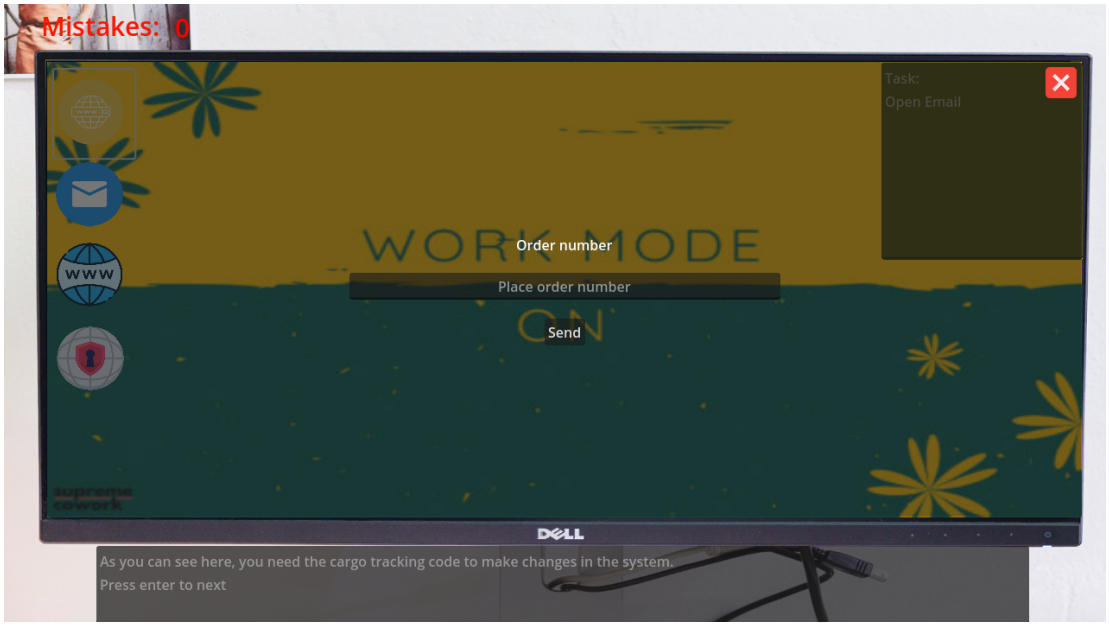

Figure 66. Game application for records

When the user finishes with the tutorial, he starts his first day. This level also opens the "Book of Knowledge," where all information related to the organization security measures and instructions is collected (see Fig. 67). Compared with other projects, this could be rephrased as integrated hints for a person. Suppose a player does not know what action to take in a specific situation. In that case, this function helps a person to take the right action from a security perspective. Some projects provide information about how to deal with social engineering attacks only one time or only at a specific time [36, 34]. In this game, users can always see the action more suitable for a particular situation.

Figure 67. Book of rules

Game days are split by different examples. Description of scenarios for days could be found in section 5.2.4 on page 75. Days go in such order: VPN access, Path change to organization webpage, Email phishing with work email, Changes in mail template, Email message link, Receive email message with prize link, Send your data, Final day. The final day scenario is not included in the chapter with a scenario description for each day. The final day level includes one example from each social engineering technique used for education in the game. Also, each time the user makes a mistake, the game will remember this, and when the user makes five mistakes, he will receive the game over the screen (see Fig. 68) and go back to the main page, but he could start the game on the level where he gets the game over. The game automatically saves player progress at the end of each level so that if the user wants to stop playing, he can finish the game later.

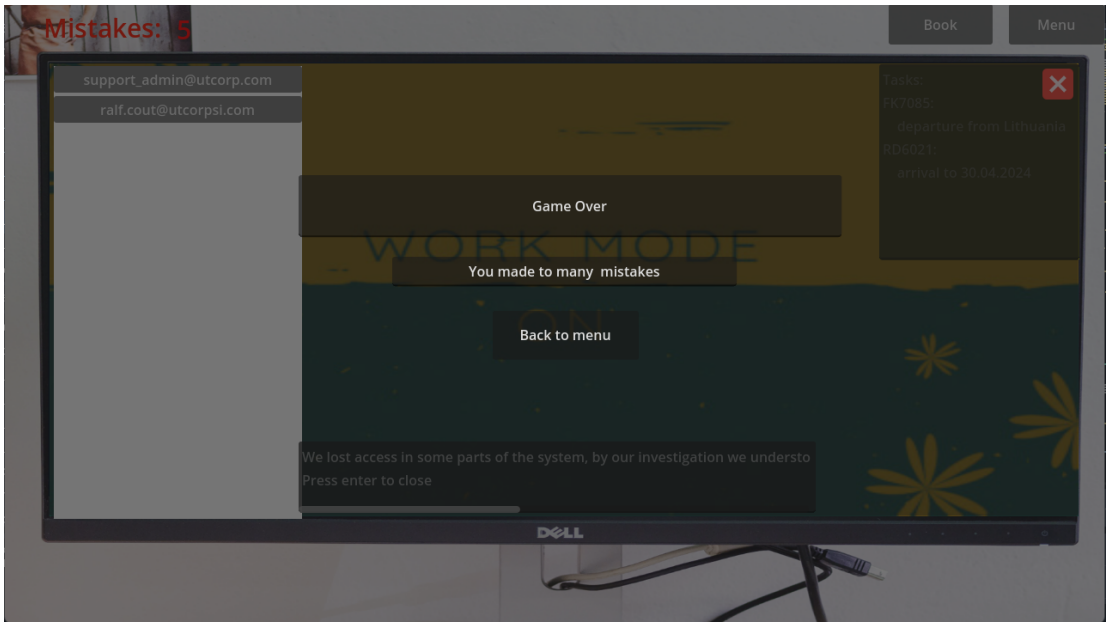

Figure 68. Game Over screen

5.3 Summary

As an answer for SRQ2 from the practical side, we created a gamified training program using information from Section 2 and data from the questionnaire from Section 4. Various tools were used for development, such as Godot as a game engine, Nuclino as a scenario application, and Figma as a UX/UI development tool and frontend creation. The agile model was chosen for testing due to its simplicity in working on small projects and its fast adaptation to development. The development process was difficult due to the author's lack of game development skills. As a result, different ideas were not included in the version used in the testing phase described in Section 6. Still, the current version provides the needed minimum of functions for testing. A more detailed description of development can be found in Section 5

6 Results of Phase-II Questionnaire

6.1 Second questionnaire

The second questionnaire provides results of how effective created training is and answers to question SRQ2 from Section 1.2 as proof of our theory about the effectiveness of a one-platform solution. The second testing phase includes a questionnaire that collects data about the experience of high school students who passed the game as a training tool to learn new knowledge and skills to mitigate social engineering attacks. The second questionnaire aims to collect data on how high school kids' skills and knowledge are improved after passing training and to collect information about their experience in playing the game to improve it. After data is collected, they would be analyzed with the first testing results.

The questions were generated and translated for the second questionnaire using ChatGPT 3.5 for time economy. The command generated questions: "Generate 10 questions for a questionnaire about social engineering techniques". Questions need to be generated later by analysis to determine whether interviewers are vulnerable to email phishing." When ChatGPT generated questions from them, they were chosen: (i) Related to the research topic; (ii) It is connected with situations in which there could be an interviewer (iii) Refrain from having technical upstarts, which could create misunderstanding of the questions for the interviewer. The same command was used to create new questions if questions were insufficient. For translation, the original text was written in English and pasted with the command "translate to 'language,'" which goes before the text. Later, the author discovered that if the author gave the text to ChatGPT in the same dialogue, he would translate the text automatically into the last provided language. Also, in the process of translation, it was found that if the person did not provide text for ChatGPT in the same dialogue for translation for a while, then he would give an answer for the text he thinks is suitable but did not translate it.

The original plan was to send email messages to people who completed the first questionnaire to receive a clear understanding of their knowledge and skills in social engineering techniques before and after they passed the training. Later, only one person from the previous group passed the game and the questionnaire. Because of that, it was decided to ask students from the same school to play a game and pass a questionnaire. Because they learn from the same school, they have the same learning program, which makes their level and skill in social engineering somewhere on the same level.

6.2 Results of second testing

In this section, the results of the second questionnaire will be described. The main idea behind the second questionnaire is to see how the skill and knowledge of respondents were raised after they had passed the created game. The second questionnaire results can

be found on page On page 95-106.

Questions 10 (see Fig. 69),11 (see Fig. 70), 13 (see Fig. 71), 15 (see Fig. 72), 17 (see Fig. 73) are related to WIPhishing. These questions are created to provide the respondents with different situations related to WIPhishing and how they deal with them. Respondents answered almost all questions right from a security perspective. Only Question 17 (see Fig. 73) shows that two people have not answered this question correctly. The question which was asked from respondents, "While traveling and using public WIFI networks, you notice that your device's battery drains much faster than usual. What would you do?". Such action as fast battery drain could happen because of usage of phone hardware resources, as an example of malicious action installed malware on the phone. In this situation, the attacker installed the user's phone program that uses phone resources to collect data through the phone when it connects to other devices. It is an active program that works all the time, and because of that, the phone uses more energy than usual. As theories why respondents answered differently from a security perspective wrongly on this question, we have two theories:

- Need to provide a little clarification about the training program. In training, they were provided information about social engineering attacks, which raised their knowledge about attacks, and training trained the user's mindset to find something wrong in the information he received. One of the key problems that could be in training is that we teach them to find problems in received information but not teach them how to use knowledge about attack work principle to identify it.

- Other questions are similar to the training exercises used in training. Because of that, respondents know how to deal with specific situations. It could be found in question 11 (see Fig. 70) where the question was "While connecting to a public WIFI network at an airport, you notice two similar network names: "Airport_Free_WIFI" and "Free_Airport_WIFI." What would you do?". Such an attack could be found in the VPN access scenario in Section 5.2.4. If such a theory is correct, then we miss something in the big picture of the project, which does not create a mindset to deal with social engineering attacks based on training and information about attacks. Still, it also provides information that the program works, and respondents have fewer chances of falling into such attacks.

Also, interesting findings could be found in tables related to age. The answers to the questions were associated with sending information about the attacks to customer support or similar roles. From the age tables, 19 year old send information about such attacks to customer support actively than other age groups. Because of a small amount of data, we cannot be sure about such a theory. Still, it could be that older people are more reliable in working with customer support to protect their surroundings.

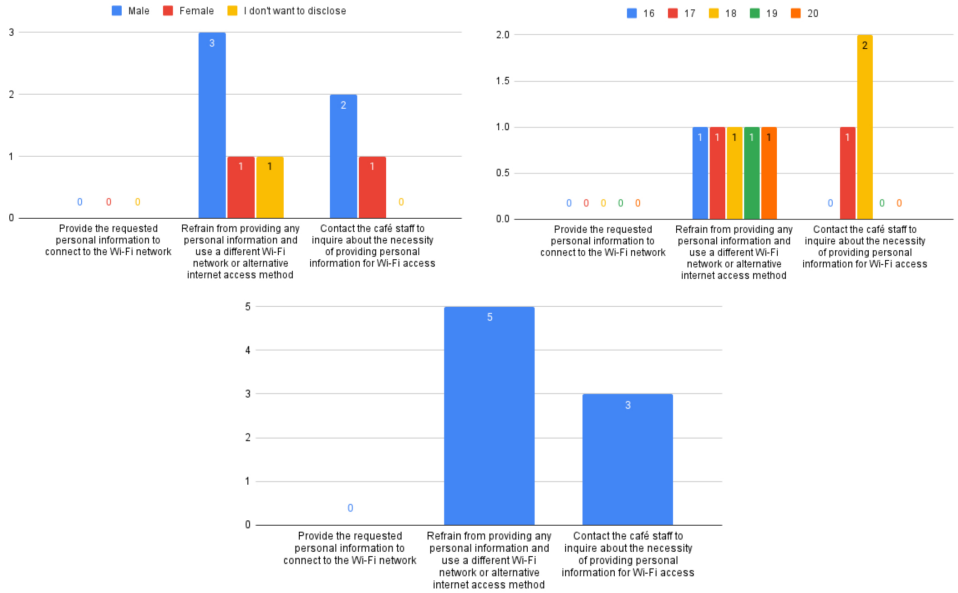

Figure 69. 10. While connecting to a public Wi-Fi network at a café, you notice that the network requires you to provide personal information such as your email address and phone number before granting access. What would you do?

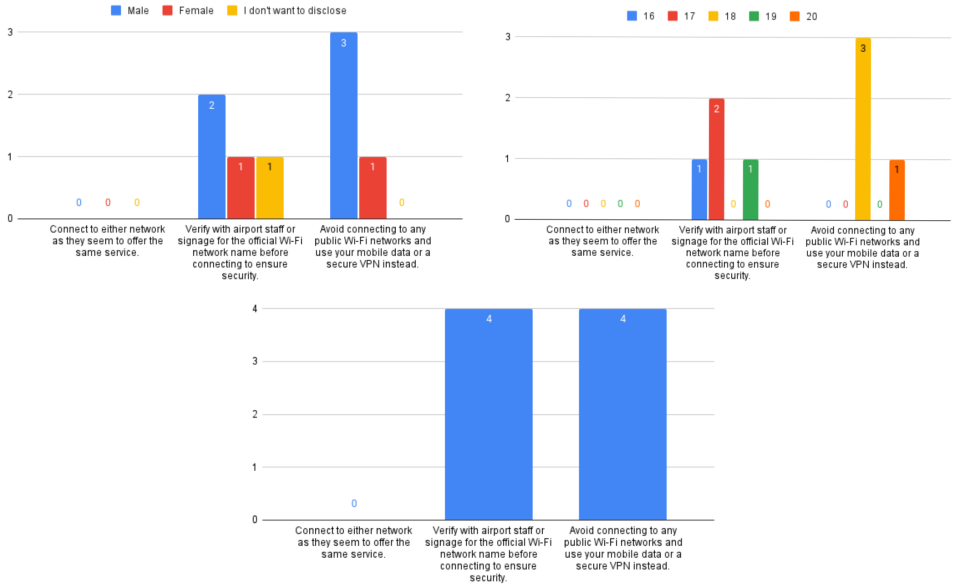

Figure 70. 11. While connecting to a public Wi-Fi network at an airport, you notice two similar network names: "Airport_Free_WIFI" and "Free_Airport_WiFi". What would you do?

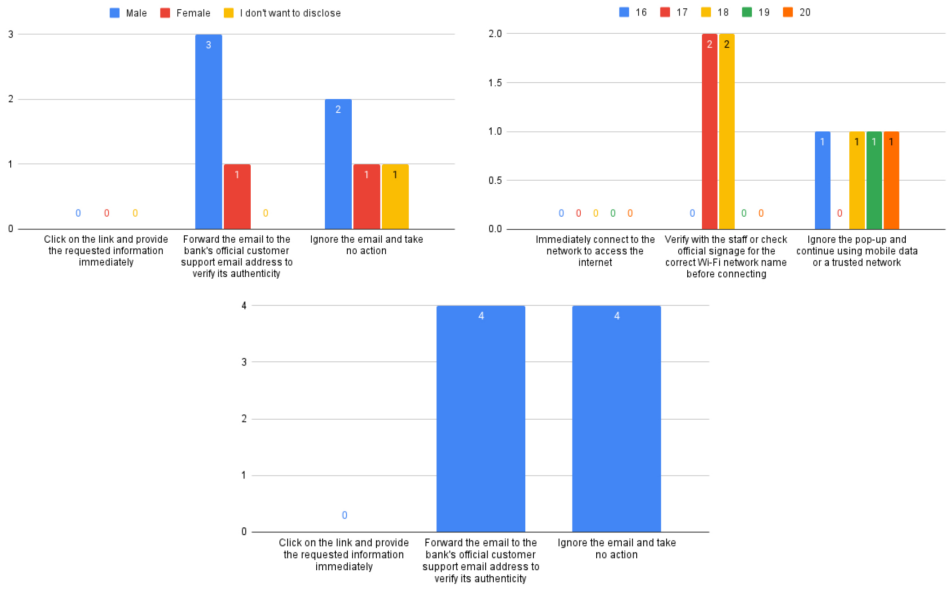

Figure 71. 13. Imagine you're in a public place with Wi-Fi access, and you receive a Pop-up notification on your device prompting you to join a network with a name similar to a popular coffee shop's Wi-Fi network. What would you do?

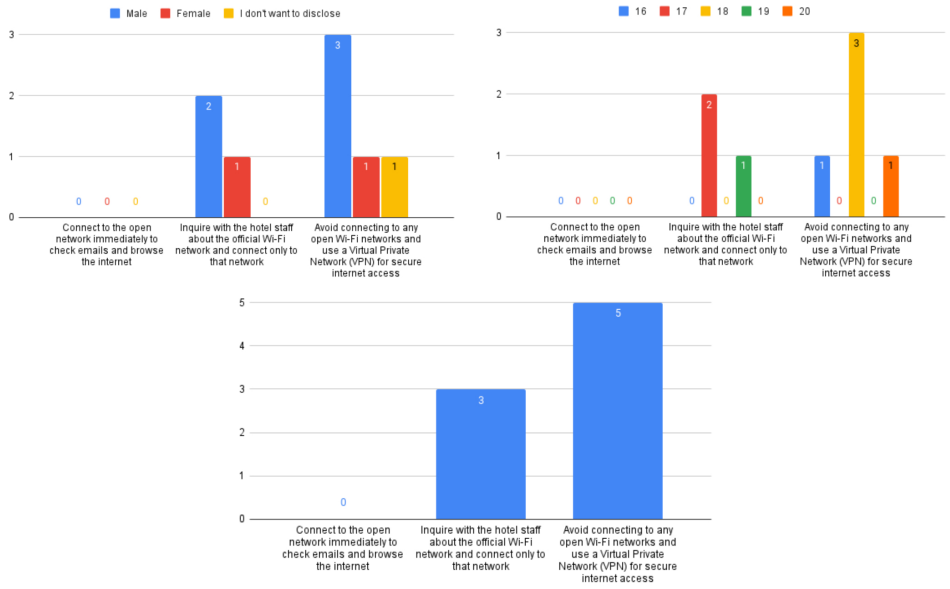

Figure 72. 15. While traveling, you notice an open Wi-Fi network with a generic name like "Free_Public_WIFI" available at your hotel. What is your next action?

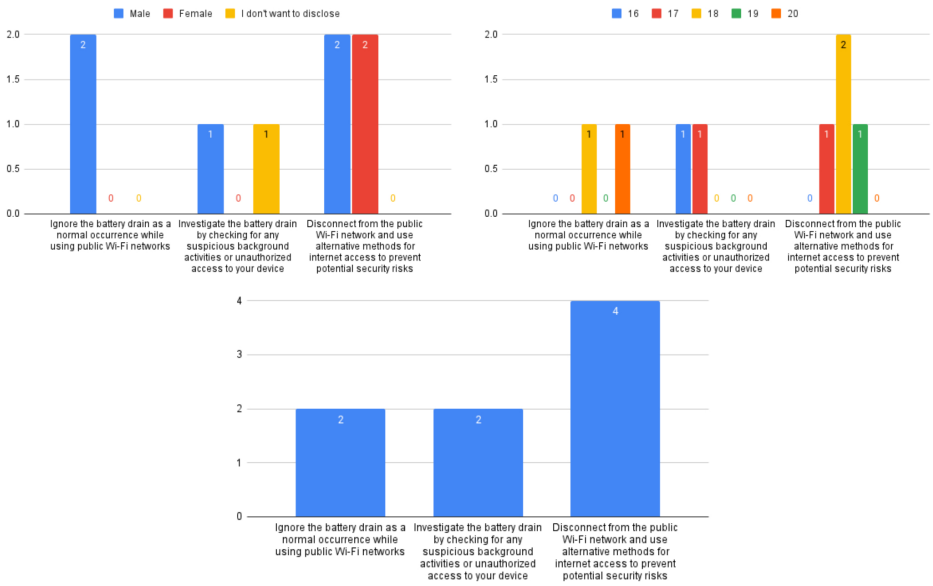

Figure 73. 17. While traveling and using public Wi-Fi networks, you notice that your device's battery drains much faster than usual. What would you do?

Questions 6 (see Fig. 74),7 (see Fig. 75), 8 (see Fig. 76), 15 (see Fig. 72), 9 (see Fig. 77), 14 (see Fig. 78), 16 (see Fig. 79), 19 (see Fig. 80), 22 (see Fig. 81) are related to Pharming. All respondents answered these questions right from a security perspective. What could be highlighted here is that respondents report incidents more actively than with WiPhishing. This could be related to situations they are dealing with in question 9 (see Fig. 77): "You receive a phone call from someone claiming to be from a tech support organization, stating that they've detected unauthorized access to your WIFI network and offering to fix it remotely. What would you do?". In this question, most respondents chose an answer to hang up the call and contact their internet provider about such a situation. Another example is question 22: "While browsing the internet, you encounter a website that claims to offer free gift cards in exchange for completing surveys and providing personal information. What would you do?". In such a situation, respondents close the website and report about it. If compared with situations from WIPhsihng, these examples could be described so that another person understands the problem and the threat from such a problem. Because of that, it would be easy to report that a more professional person understands it and if it is something bad or not. Now, if we look at the age table, most reports are from respondents aged 18. This finding supports our theory from WIPhishng that age could be a factor for reporting incidents related to social engineering, but for that, we could also add simplicity in providing information about the incidents.

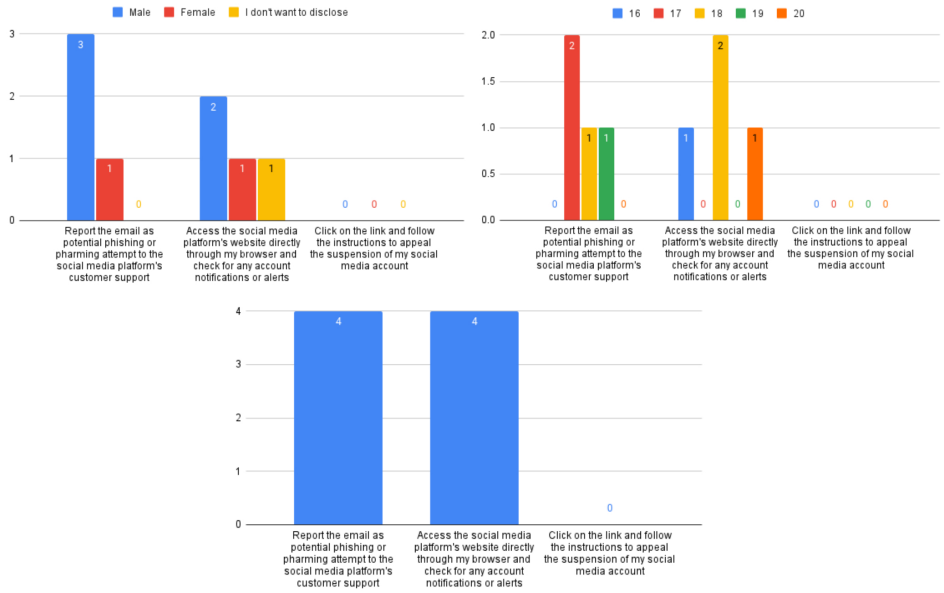

Figure 74. 6. You receive an email from a well-known social media platform, informing you that your account has been suspended due to a violation of their terms of service and asking you to click on a link to appeal the suspension. How would you proceed?

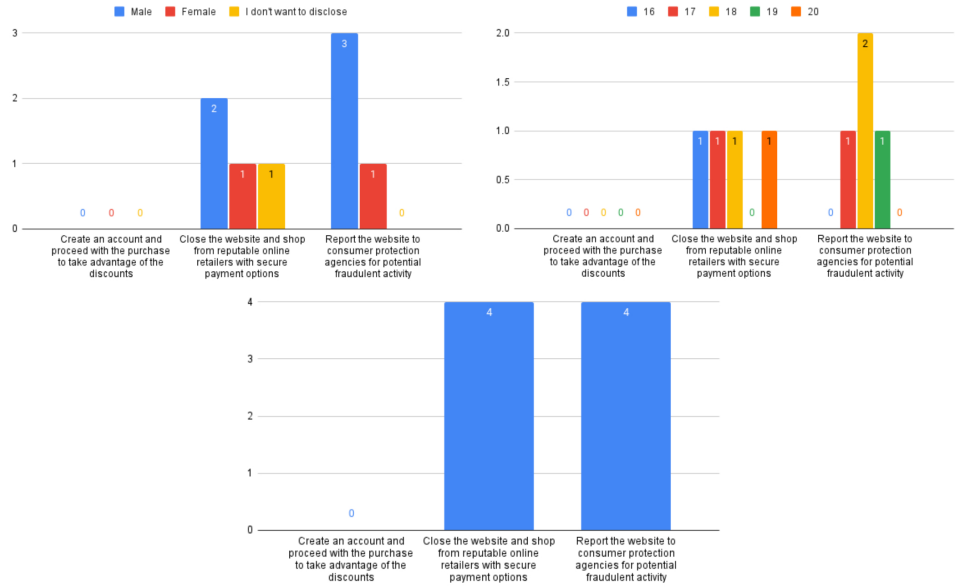

Figure 75. 7. While shopping online, you encounter a website that offers significant discounts on luxury items but requires you to create an account with your personal information before making a purchase. What would you do?

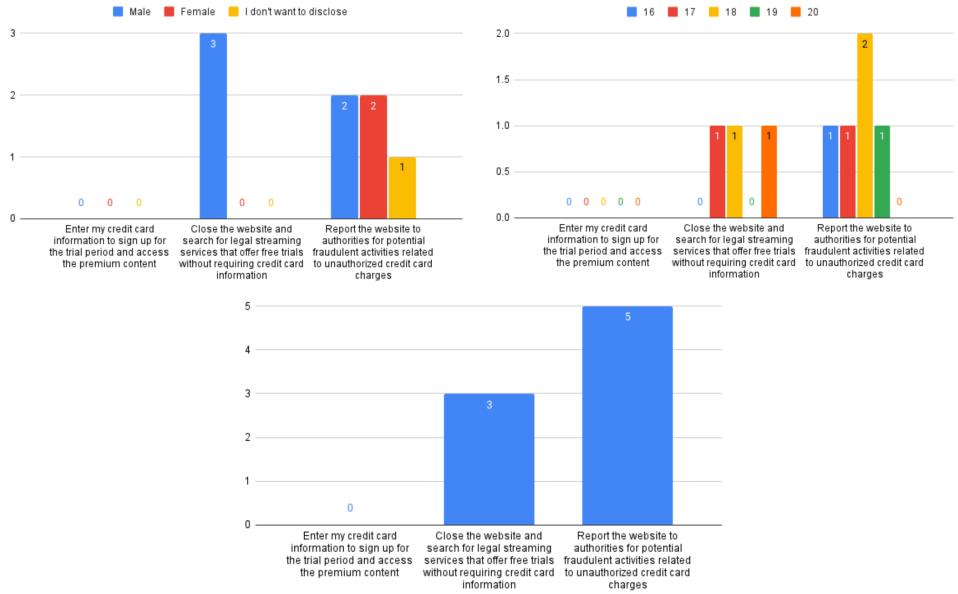

Figure 76. 8. While browsing the internet, you come across a website that claims to offer free access to premium movies and TV shows but requires you to enter your credit card information to sign up for a trial period. What would you do?

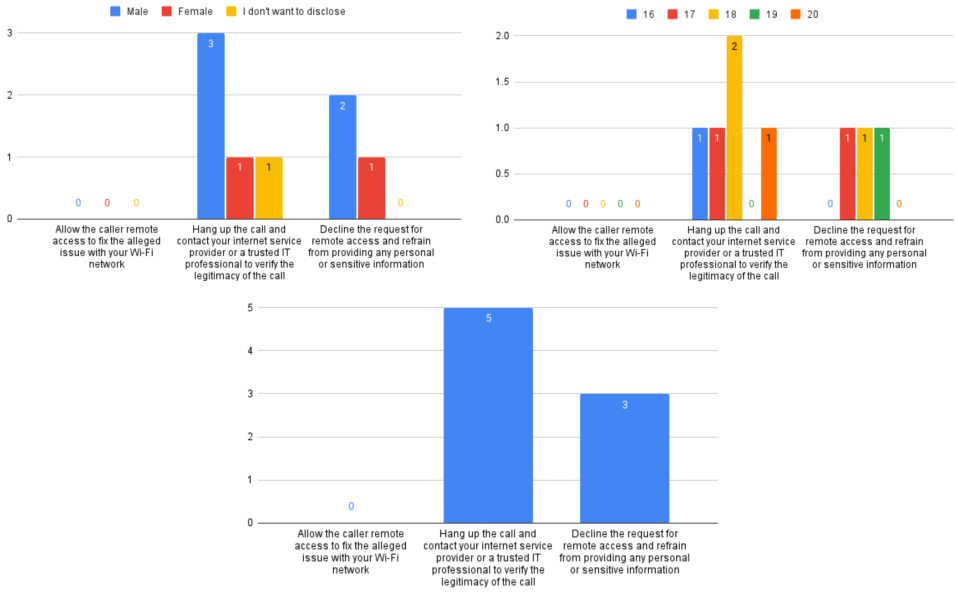

Figure 77. 9. You receive a phone call from someone claiming to be from a tech support organization, stating that they've detected unauthorized access to your Wi-Fi network and offering to fix it remotely. What would you do?

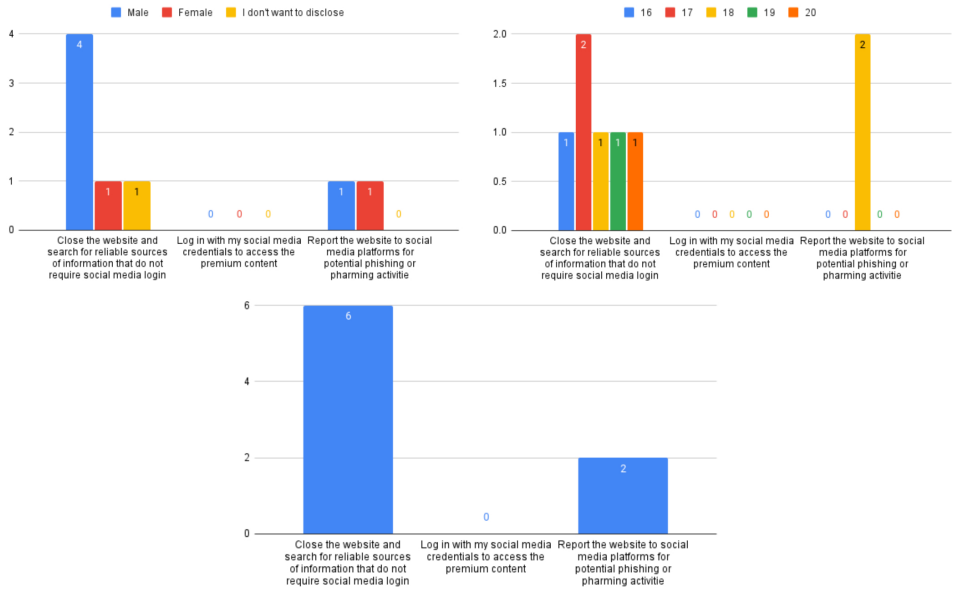

Figure 78. 14. While searching for information online, you come across a website that claims to provide free access to premium content but requires you to log in with your social media credentials. What would you do?

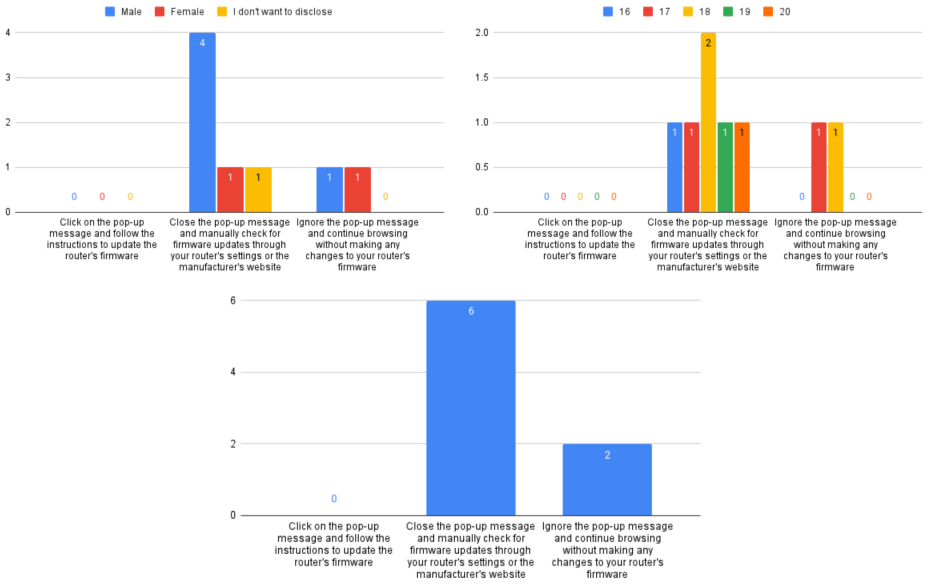

Figure 79. 16. While browsing the internet on your laptop, you encounter a Pop-up message claiming that your Wi-Fi router's firmware is outdated and needs to be updated immediately. What would you do?

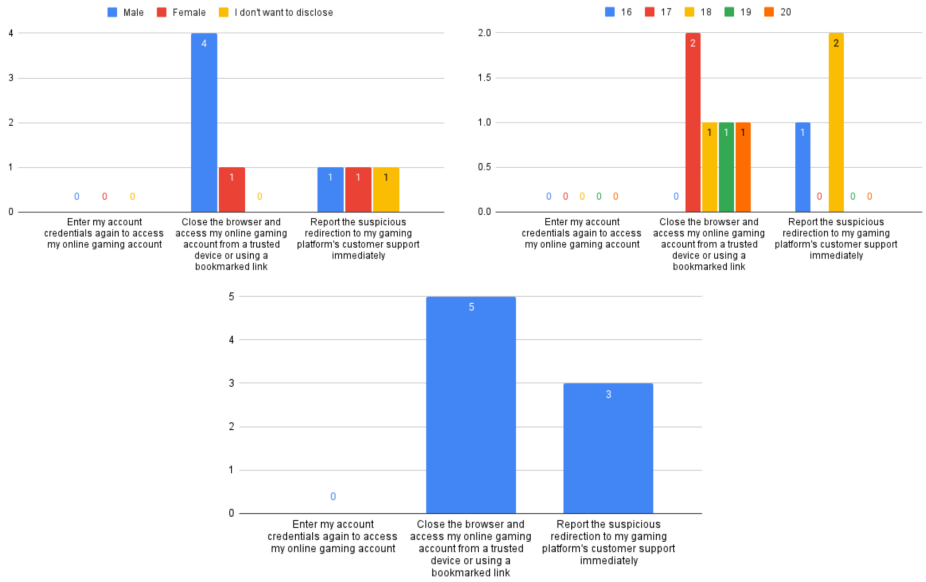

Figure 80. 19. While attempting to access your online gaming account, you're redirected to a page that asks for your account credentials again, claiming that there's been a security update. What would you do?

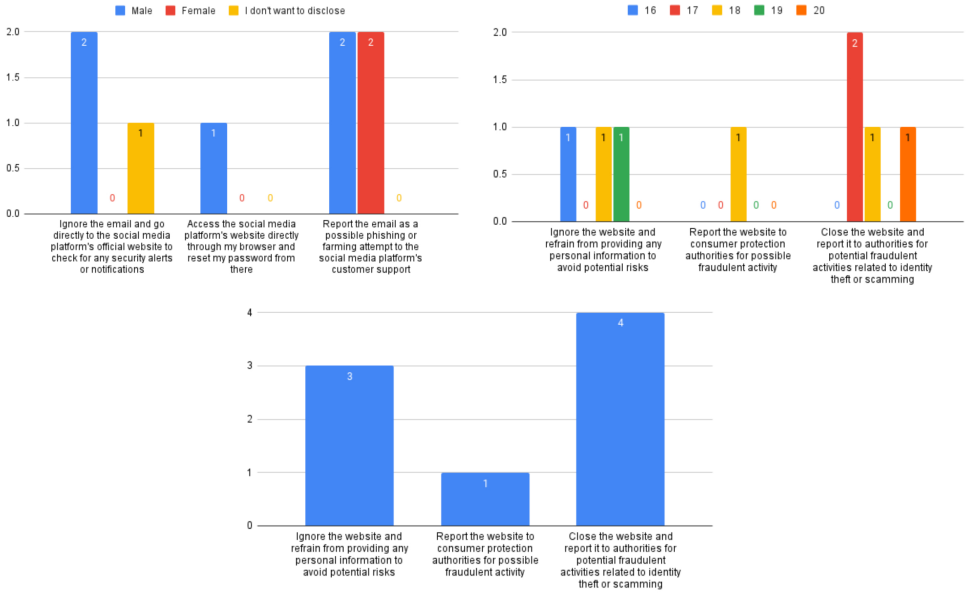

Figure 81. 22. While browsing the internet, you encounter a website that claims to offer free gift cards in exchange for completing surveys and providing personal information. What would you do?

Questions 12 (see Fig. 82),18 (see Fig. 83), 20 (see Fig. 84), 21 (see Fig. 85), 23 (see Fig. 86), 24 (see Fig. 87), 25 (see Fig. 88), 26 (see Fig. 89) are related to Email Phishing. Questions 12, 18, 20, and 21 contain situations and answers. Questions 23, 24, 25, and 26 are questions where respondents must choose the right picture or answer whether an email is fake or true. Let us start with questions with answers. From a security perspective, all responders answered the right questions. Interestingly, in question 20 (see Fig. 84), "You receive an email from a social media platform informing you that your account has been compromised and requires immediate action. The email contains a link to reset your password. How would you proceed?". Most respondents access social media platforms and change their passwords in this situation. This indicates that respondents like to secure something valuable for them; in this situation, this is information. The same pattern could be seen in question 18: "You receive an email from a friend with an attachment labeled as "Important Document." However, the email seems out of character for your friend, and you suspect it might be a phishing attempt. What do you do?". Even if an email message was not sent to them, respondents sent messages to their friends about the attack to warn them about it. It is the same as in question 20; something valuable, but valuable for this situation, means connections with people close to respondents. This supports the early theory that one of the best tactics for teaching about social engineering is to provide threats that could affect something valuable to a person and teach them to act on the situation.

Now, we move to questions with pictures. Questions 23(see Fig. 86) and 24 (see Fig. 87) were provided pictures with email messages from which respondents needed to choose the right one. Results from question 23 (see Fig. 86) were the same once, but in question 24 (see Fig. 87), most respondents chose option 3, which was the right one. Still, some respondents in question 24 (see Fig. 87) chose the wrong answers. Such data could support the theory that respondents do not find information about the correct email address because of the teaching method. The training exercises provide all the information necessary for passing social engineering attacks. Still, such training makes them work in a "black box" or closed environment, which does not train their skills to find information not included in the training. Because of the data from questions 23 (see Fig. 86) and 24 (see Fig. 87), they try to figure it out by finding key points they know. They can identify it by parameters such as wrong name, email, characters they already know, etc. This theory could support questions 25 (see Fig. 88) and 26 (see Fig. 89) where needed to provide the answers if the email was valid or fake, and they have a similar pattern with questions 23 (see Fig. 86) and 24 (see Fig. 87). In question 25 (see Fig. 88), we have the same results in real and fake answers; in question 26 (see Fig. 89), most respondents chose fake, which was the correct answer.

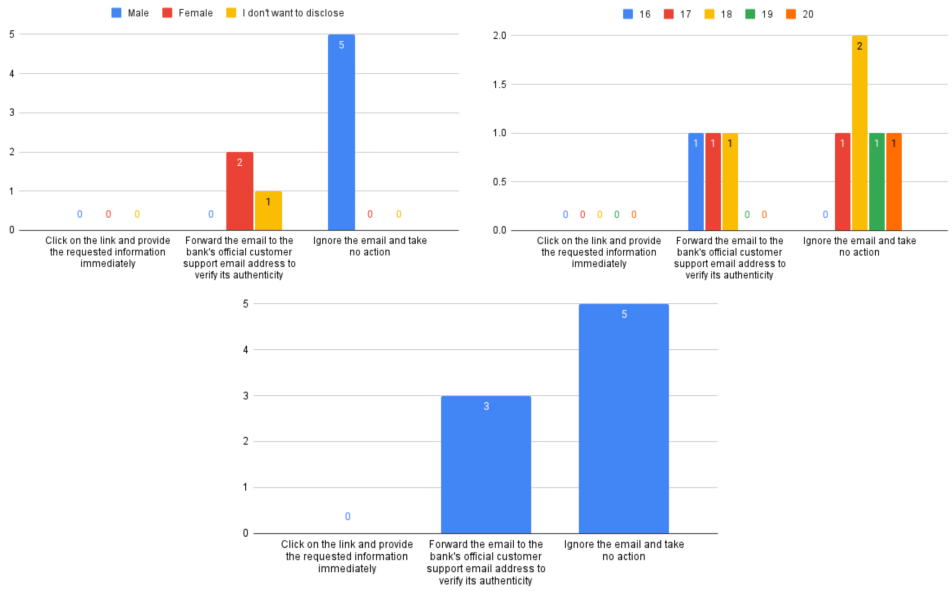

Figure 82. 12. Imagine you receive an email from your bank stating that your account has been compromised, and you need to click on a link to verify your information urgently. What would you do?

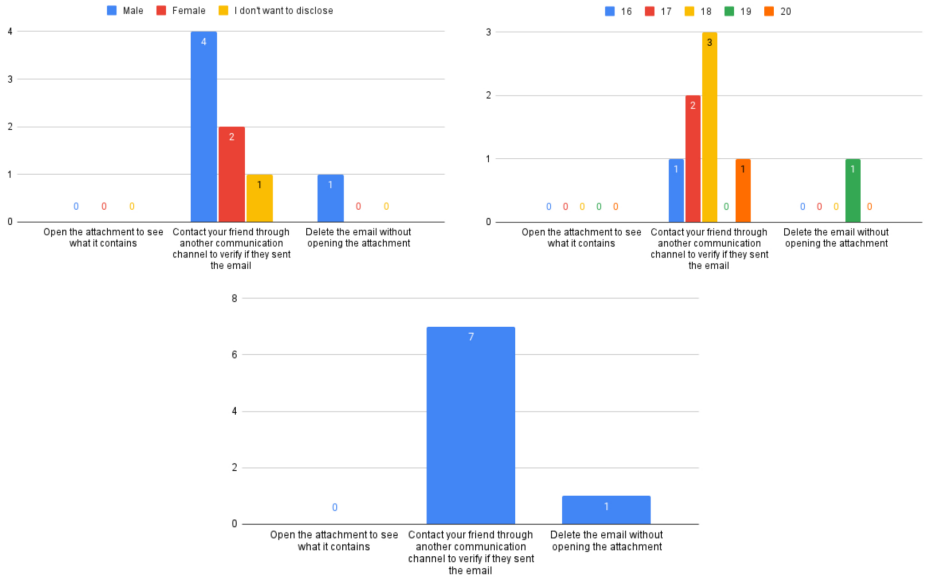

Figure 83. 18. You receive an email from a friend with an attachment labeled as "Important Document." However, the email seems out of character for your friend, and you suspect it might be a phishing attempt. What do you do?

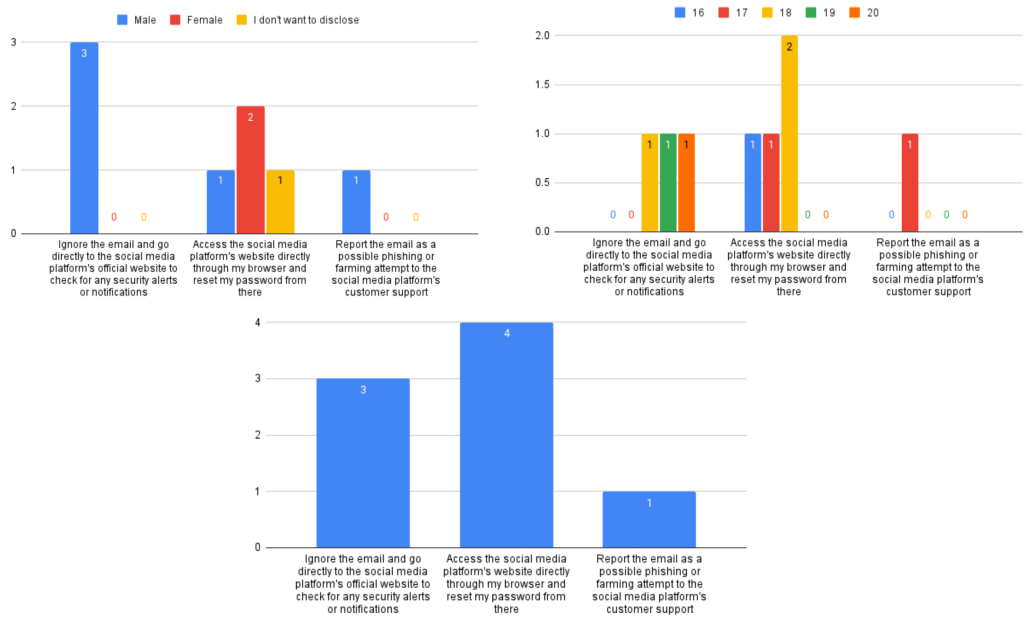

Figure 84. 20. You receive an email from a social media platform informing you that your account has been compromised and requires immediate action. The email contains a link to reset your password. How would you proceed?

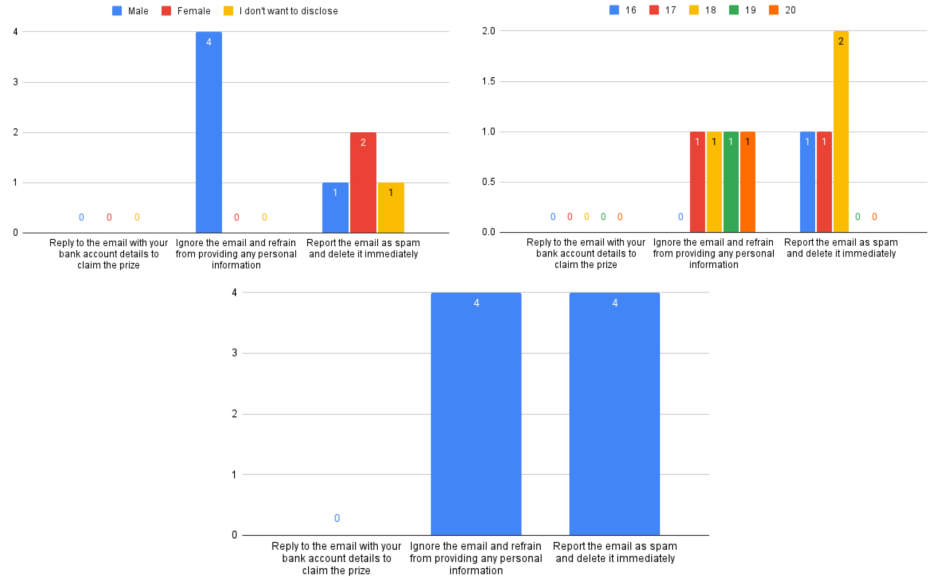

Figure 85. 21. You receive an email with a subject line stating that you've won a lottery, and you need to provide your bank account details to claim the prize. What do you do?

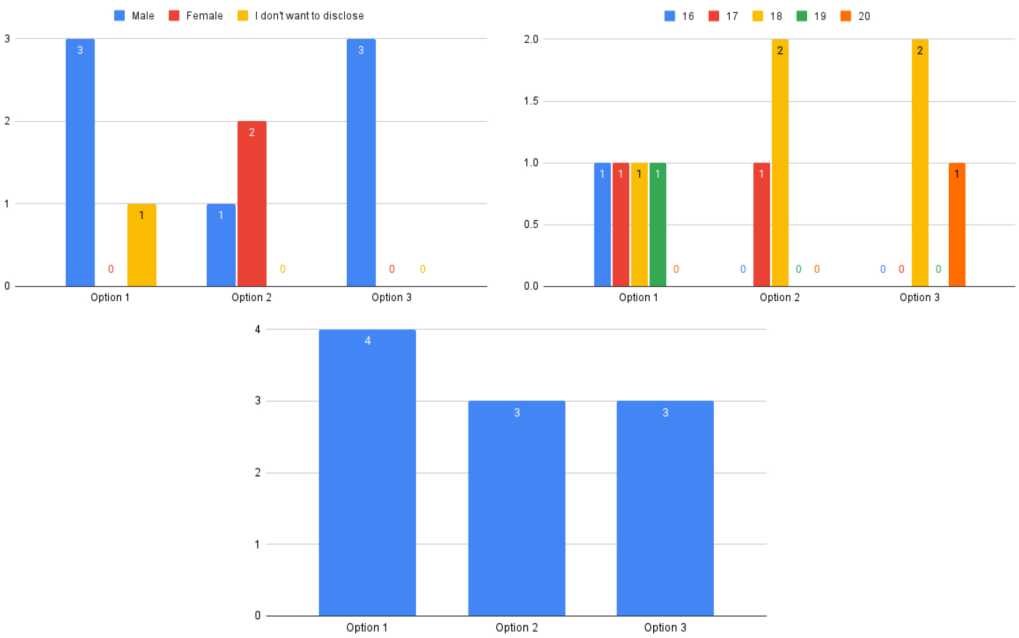

Figure 86. 23. Which one is true email?

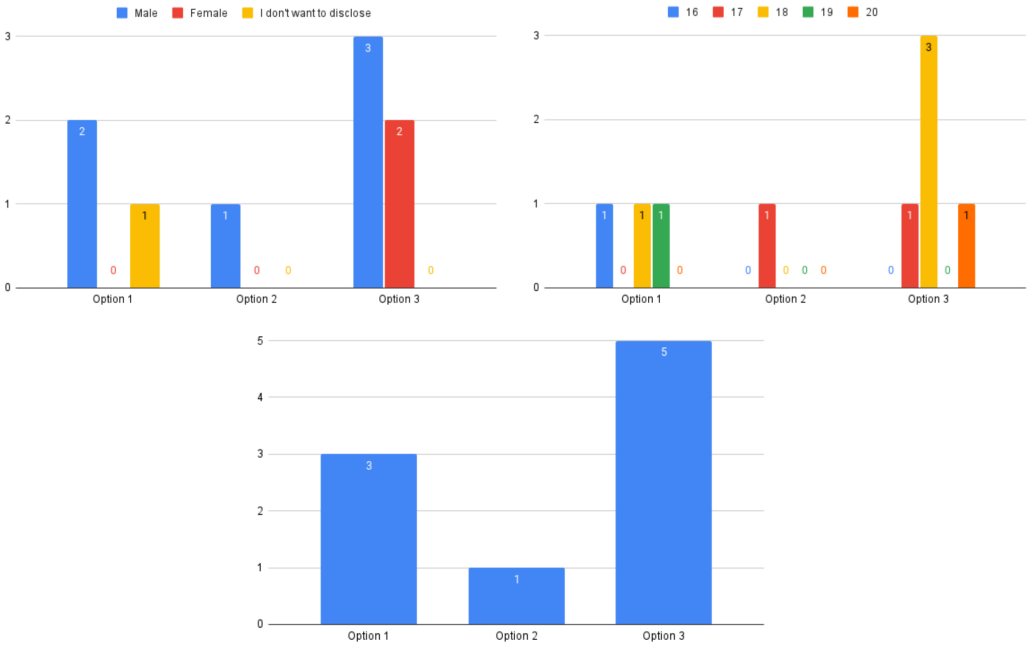

Figure 87. 24. Which one is true email?

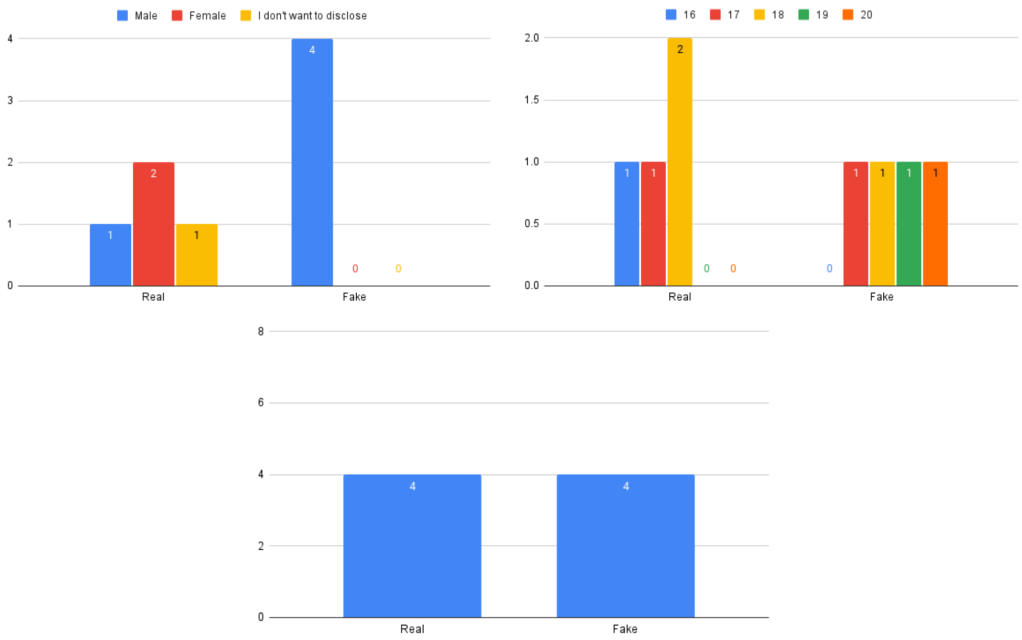

Figure 88. 25. Is this a real email or fake?

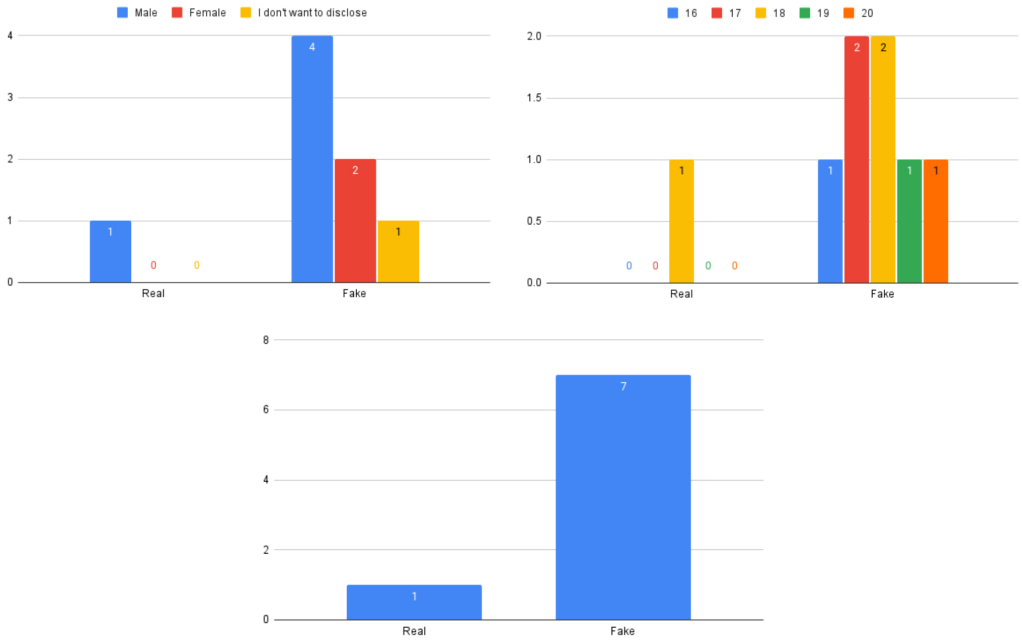

Figure 89. 26. Is this a real email or fake?

Summarizing all information from the second questionnaire, respondents understand how to deal with social engineering attacks through tasks provided in the training program but could not create for themselves a proper mindset for social engineering mitigation using knowledge and skills. If we compare results in Section 4.2 about Email phishing, Pharming, and WIPhishing, we could see improvement in dealing with tasks related to the above topics. For example, answers to the questions associated with Pharming show that high school students who passed training almost all answered questions correctly from a security perspective (as an example, see Fig. 74, Fig. 75, Fig. 76). Still, in Email phishing and WIPhishing, it could be seen that respondents still make mistakes in these topics. Understandably, not all respondents answer on topics 100 percent correctly, and based on the received results, there could be a margin of error. But results from email phishing questions 23 (see Fig. 86), 24 (see Fig. 87), 25 (see Fig. 88), 26 (see Fig. 89) show that respondents struggle to identify correct email from the list. The provided data also show that in most cases, 18- and 20-year-old respondents reported social engineering attacks more actively than younger-age respondents. Also, in email phishing graphs (as example see Fig. 69) we see that understanding the topic and providing information in the correct form raises the chance that younger respondents report the incident actively. As for gender differences in answers from the results of the questionnaire, males less actively report social engineering threats to organizations or persons that are related to platforms where the attack happens. It is shown on graphs related to Pharming (as an example, see Fig. 82 and Email phishing (as an example, see Fig. 74. At last, respondents provided positive feedback about the game education process but highlighted problems with the design. In the questionnaire, was asked for feedback about the game. Respondents offered positive feedback about social engineering techniques and simple gameplay, which educated them about topics in the game. From the minuses, respondents provide that the game looks raw in graphics.

6.3 Summary

After passing the created training, the second questionnaire provided data about changes in high school students social engineering knowledge and skills. Changes could be seen in all techniques provided in the questionnaire. Still, in some situations, respondents have problems with social engineering techniques not from knowledge but from practical skills. It can be seen in Email phishing exercises related to pictures of emails. Theoretically, it could be due to a lack of training exercises related to different variations of the same problem for better memorizing material. This could be found by an analysis of the current version of training and future updates and testing. Still, the results show a positive impact, which could prove our methods for developing one solution platform for research question SRQ2.

7 Conclusion

This thesis is written to provide information about current problems and gaps in knowledge of social engineering techniques among high school students and how they could be solved by providing one-platform solution training. While finding key elements of the problem in the topic, it was found that high school students know little about social engineering and how it works, affecting their ability to recognize and mitigate threats. Still, high school students' ability to find something new for themselves also helps them find information about popular social engineering attacks and, in the future, helps them to mitigate them, even if they do not know that it is a social engineering attack. Still, as shown by the results of the second questionnaire, training on topics such as social engineering helps provide knowledge and skills for mitigating future attacks. Even if our training did not provide results as expected, it still had positive results and feedback, which showed that we were on the right path.

7.1 Answer to research questions

By working on this thesis, we try to answer the research question "How to educate school students about social engineering techniques" using a one-platform solution. As a result, we found answers to our research questions described in Section 1.2:

SRQ1: By the provided results from the first questionnaire, high school students are vulnerable to social engineering techniques which are related to using technical instruments such as creating fake websites, providing documents masked as viruses, and using free WIFI hotspots for collecting traffic from users. An opposite attack, which requires contact respondent inject percentage, is low. By received answers, this could happen because of: (i) a low level of knowledge about social engineering techniques and how they work on a fundamental level; (ii) social engineering attacks that require speaking with a person raised in popularity by an attacker. Because of that, respondents could be in a situation where they were the target of such an attack or hear about it from social media or a story about it.

SRQ2: The thesis described methods of implementing training using the human-centered approach for better assimilation of information by a person who passes training and acquires skills to mitigate the attack. Also, it was discussed which training approach to take to provide training in an interactive format so that the person who passes it could learn from his mistakes and find ways to pass specific training steps differently. As a result, gamified training was created, which put practical exercises at the game's core, which required information analysis. The person who passes training trains their analytical skills, and using information about social engineering attacks in the future helps to be attentive to the information he works with. More information about training methods can be found in Sections 2.2, 2.3, and 2.4, and about a one-platform solution can be found in Section 5.

We tested our training program and one-platform solution on high school students to validate our training program. The first questionnaire was created to understand the situation with social engineering techniques among high school students. The second questionnaire was used to validate the training. Results can be found in chapters 4 and 6. If we compare results before and after training, we could highlight that training helped to receive skills in analyzing situations from training. However, with cases that require validating the information by finding it themselves, high school students still need help. Also, the first and second questionnaires highlight that high school students become more aware of the information they receive when it could affect something vital to them. It could be money, connections, or something important to them. Because our respondents are high school students, they have a long way to go in their life path. When something could affect their connections or belongings, they could pay more attention to it.

7.2 Limitations

Because the thesis data were collected only from Narva town, this thesis does not provide information about the situation in other Estonian regions. Also, because this thesis has limited time, it chose only specific social engineering techniques with which interviewers from the first questionnaire had problems. In such a way, information about other social engineering techniques is not provided to the target audience, making them vulnerable to such techniques. Also, as was said earlier, the game was not completed the way planned, which provided a less fun experience and immersion in situations related to social engineering techniques.

7.3 Future works

First of all, data from other Estonian regions need to be collected to understand better situations related to social engineering techniques. Also, we need to test our theory about the effect of personal belongings on decision-making related to the analysis of social engineering. Because we have data only from Narva, we could highlight some theories about how high school students deal with social engineering. Still, for a better understanding, we require more data.

Also, need to analyze the current version of the game in more detail and understand why training has not worked as planned. As was said earlier by the second questionnaire, respondents still have problems with the analysis of social engineering attacks, which require finding information from external sources. Also, new data about personal satisfaction with the current model of the game needs to be collected to change or add elements that could make a game a better instrument for teaching social engineering. As a modification for the training instrument, we need to add functionality that could upload modules for the base game. Because the game is a one-platform solution for training, adding new exercises to the game is required. It could be done by coding it into a game,

but not everyone knows how to code. It will help to integrate new exercises and open a game for people who like to use it for education about social engineering.

References

[1] Raza M. Abdulla, Hiwa A. Faraj, Choman O. Abdullah, Askandar H. Amin, and Tarik A. Rashid. Analysis of social engineering awareness among students and lecturers. *IEEE Access*, 11, 2023.

[2] Fadi Abu-Amara, Reem Almansoori, Safa Alharbi, Marwah Alharbi, and Asma Alshehhi. A novel seta-based gamification framework to raise cybersecurity awareness. *International Journal of Information Technology*, 13:2371–2380, 12 2021.

[3] Samar Muslah Albladi and George R.S. Weir. User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*, 8, 2018.

[4] Hussain Aldawood and Geoffrey Skinner. An advanced taxonomy for social engineering attacks. *International Journal of Computer Applications*, 177, 2020.

[5] Bandar S. Almutairi and Abdurahman Alghamdi. The role of social engineering in cybersecurity and its impact. *Journal of Information Security*, 13, 2022.

[6] Abdullah M. Alnajim, Shabana Habib, Muhammad Islam, Hazim Saleh Al-Rawashdeh, and Muhammad Wasim. Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches. *Symmetry*, 15:2175, 12 2023.

[7] Maher Alsharif, Shailendra Mishra, and Mohammed AlShehri. Impact of human vulnerabilities on cybersecurity. *Computer Systems Science and Engineering*, 40, 2021.

[8] and European Union Institute for Security Studies, S Secrieru, and N Popescu. *Hacks, leaks and disruptions – Russian cyber strategies*. Publications Office, 2018.

[9] Ruth Korede Ayeni, Ayodele Ariyo Adebiyi, Julius Olatunji Okesola, and Ennmanuel Igbekele. Phishing attacks and detection techniques: A systematic review. In *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG)*, pages 1–17. IEEE, 4 2024.

[10] Marina Begunkova. Bought fast food for 2 euros - lost 100 and didn't even eat! fraudsters are operating on behalf of mcdonald's. *https://rus.delfi.ee/statja/120265285/kupil-fastfud-za-2-evro-lishilsya-100-i-dazhe-ne-poel-ot-imeni-mcdonald-s-oruduyut-moshenniki*, 1 2024.

[11] Chandra Sekhar Bhusal. Systematic review on social engineering: Hacking by manipulating humans. *Journal of Information Security*, 12, 2021.

[12] Jacek Bil. The russian social engineering attack on the president of the republic of poland as a manifestation of modern soft power. *Przegląd Nauk o Obronności*, 11 2020.

[13] Nabin Chowdhury, Sokratis Katsikas, and Vasileios Gkioulos. Modeling effective cybersecurity training frameworks: A delphi method-based study. *Computers Security*, 113:102551, 2 2022.

[14] Devfuzion. Smishing: What you need to know about text scams. `https://www.devfuzion.com/smishing-what-you-need-to-know-about-text-scams/`, 2020. [Online; accessed 30-November-2024].

[15] Jill Dougherty and Riina Kaljurand. Estonia's "virtual russian world": The influence of russian media on estonia's russian speakers, 2015.

[16] Ahlam Fakieh and Aymen Akremi. An effective blockchain-based defense model for organizations against vishing attacks. *Applied Sciences*, 12:13020, 12 2022.

[17] Adrien Gendre. Bec scam: How to avoid becoming a victim. `https://www.vadesecure.com/en/blog/bec-scam-how-to-avoid-becoming-a-victim`, 2020. [Online; accessed 30-November-2024].

[18] Marthie Grobler, Raj Gaire, and Surya Nepal. User, usage and usability: Redefining human centric cyber security. *Frontiers in Big Data*, 4, 3 2021.

[19] Christopher Hadnagy. *Social engineering: The art of human hacking*. John Wiley & Sons, 2010.

[20] Richard Harte, Liam Glynn, Alejandro Rodríguez-Molinero, Paul MA Baker, Thomas Scharf, Leo R Quinlan, and Gearóid ÓLaighin. A human-centered design methodology to enhance the usability, human factors, and user experience of connected health systems: A three-phase methodology. *JMIR Human Factors*, 4:e8, 3 2017.

[21] Sriendra Deshan Ilangakoon and K.Y. Abeywardena. The use of subliminal and supraliminal messages in phishing and spear phishing based social engineering attacks; feasibility study. pages 1–5. IEEE, 8 2018.

[22] ISO. Human-centred design for interactive systems. 2010.

[23] Jovana Karać and Martin Stabauer. *Gamification in E-Commerce*. 2017.

[24] Katalon. Agile testing methodology: A complete guide for agile testers. https://katalon.com/resources-center/blog/agile-testing-methodology, 2023. [Online; accessed 12-May-2024].

[25] Khoros. The 6-step social media risk management plan. https://khoros.com/blog/6-step-plan-implementing-social-media-risk-management-solution, 2023. [Online; accessed 30-November-2024].

[26] Barbora Kotkova and Martin Hromada. The threat of social engineering and the safety of companies. pages 126–133. IEEE, 7 2021.

[27] Olga Kulyk, Robert Kosara, Jaime Urquiza, and Ingo Wassink. *Human-Centered Aspects*, pages 13–75. Springer Berlin Heidelberg.

[28] Pavel Y. Leonov, Alexander V. Vorobyev, Anastasia A. Ezhova, Oksana S. Kotelyanets, Aleksandra K. Zavalishina, and Nikolay V. Morozov. The main social engineering techniques aimed at hacking information systems. 2021.

[29] Theodore Longtchi, Rosana Montañez Rodriguez, Laith Al-Shawaf, Adham Atyabi, and Shouhuai Xu. Internet-based social engineering attacks, defenses and psychology: A survey, 2022.

[30] Fitri Marisa, Sharifah Sakinah, Zeratul Izzah, Anastasia L, Ronald David, and Anang Aris. Evaluation of student core drives on e-learning during the covid-19 with octalysis gamification framework. *International Journal of Advanced Computer Science and Applications*, 11, 2020.

[31] Rob J. Nadolski, Hans G. K. Hummel, Henk J. van den Brink, Ruud E. Hoefakker, Aad Slootmaker, Hub J. Kurvers, and Jeroen Storm. Emergo: A methodology and toolkit for developing serious games in higher education. *Simulation Gaming*, 39:338–352, 9 2008.

[32] James Nicholson, Yousra Javed, Matt Dixon, Lynne Coventry, Opeyemi Dele Ajayi, and Philip Anderson. Investigating teenagers' ability to detect phishing messages. 2020.

[33] Wilk Oliveira, Armando M. Toda, Paula T. Palomino, Luiz Rodrigues, and Seiji Isotani. Which one is the best? a quasi-experimental study comparing frameworks for unplugged gamification. *RENOTE*, 18, 2020.

[34] Barack Onduto. Gamification of cyber security awareness – a systematic review of games. 1 2021.

[35] Yogesh Patel, Sudeep Tanwar, Rajesh Gupta, Pronaya Bhattacharya, Innocent Ewean Davidson, Royi Nyameko, Srinivas Aluvala, and Vrince Vimal. Deepfake generation and detection: Case study and challenges. *IEEE Access*, 11:143296–143323, 2023.

[36] Hani Qusa and Jumana Tarazi. Cyber-hero: A gamification framework for cyber security awareness for high schools students. pages 0677–0682. IEEE, 1 2021.

[37] Md Lutfor Rahman, Daniel Timko, Hamid Wali, and Ajaya Neupane. Users really do respond to smishing. In *Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy*, CODASPY '23, page 49–60, New York, NY, USA, 2023. Association for Computing Machinery.

[38] Fatima Salahdine and Naima Kaabouch. Social engineering attacks: A survey. *Future Internet*, 11:89, 4 2019.

[39] Wenni Syafitri, Zarina Shukur, Umi Asma Mokhtar, Rossilawati Sulaiman, and Muhammad Azwan Ibrahim. Social engineering attacks prevention: A systematic literature review. *IEEE Access*, 10, 2022.

[40] Cyber Writes Team. What is qr code phishing? (quishing) – attack prevention guide in 2024. `https://sosafe-awareness.com/glossary/phishing/`, 2024. [Online; accessed 30-November-2024].

[41] O. Toutsop. A capstone project: Designing an iot threat modeling to prevent cyber-attacks. *2021 Fall ASEE Middle Atlantic Section Meeting*.

[42] P. Unchit, S. Das, A. Kim, and L. J. Camp. Quantifying susceptibility to spear phishing in a high school environment using signal detection theory. volume 593 IFIPAICT, 2020.

[43] Timothy Vidas, Emmanuel Owusu, Shuai Wang, Cheng Zeng, Lorrie Faith Cranor, and Nicolas Christin. *QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks*, pages 52–69. 2013.

[44] Wikipedia. Scareware. `https://en.wikipedia.org/wiki/Scareware`, 2024. [Online; accessed 30-November-2024].

[45] Bojia Zi, Minghao Chang, Jingjing Chen, Xingjun Ma, and Yu-Gang Jiang. Wilddeepfake. In *Proceedings of the 28th ACM International Conference on Multimedia*, pages 2382–2390. ACM, 10 2020.

[46] Ömer Aslan, Semih Serkant Aktuğ, Merve Ozkan-Okay, Abdullah Asim Yilmaz, and Erdal Akin. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions, 3 2023.

II. Licence

Non-exclusive licence to reproduce thesis and make thesis public

I, **Santeri Rikhard Artturi Pohjaranta**

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to

   reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

   Developing a Human-Centric Training Method to Educate High School Students on Social Engineering Techniques

   supervised by Dr. Mubashar Iqbal.

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Santeri Rikhard Artturi Pohjaranta
09/01/2025