Touched ICT Topics - PhishGuard

Authors: Roko Mladinić, Daniella Namuli, Simeon Markov, Zed Minabowan

Introduction

This document describes three ICT topics that were used during the development of the PhishGuard game and explains how we oriented ourselves and how each ICT topic was applied in the game. We combined technical skills with cybersecurity in order to create an interactive learning experience. This document focuses on Cybersecurity, Software Engineering and Game Development.

ICT Topics we touched

1. Cybersecurity

Description

Cybersecurity was a core topic in our project because the game focuses on teaching users how to recognize phishing attacks. Phishing is a common cyber threat where attackers try to trick users into giving away sensitive information such as passwords or personal data. Understanding how attackers think and operate was essential to creating realistic phishing scenarios for the game.

Orientation Process

We oriented ourselves in this topic by researching different types of phishing attacks, such as email phishing, fake login pages and fraud techniques. We analysed real-world phishing examples and identified common red flags like urgency, suspicious links and generic messages. This research helped us design believable phishing scenarios and make the game educational as well as realistic.

Application in the Project

The knowledge gained was used to create phishing examples like fake emails and login pages within the game. Players are challenged to detect these attacks and learn how to respond safely, making cybersecurity awareness the main learning goal of the project.

2. Software Engineering

Description

Software engineering played an important role in building the actual game. This included structuring the application, creating pages and implementing the login system. We used technologies like html, TailwindCSS, typescript, Nuxt, JavaScript, Vue, PostgreSQL database to turn our ideas into a working digital product.

Orientation Process

We oriented ourselves by learning the basics of Nuxt and Vue and focusing on how pages are structured and how components work together. We explored existing tutorials and documentation to understand routing, page creation and how assets like images and logos are used in a project.

Application in the Project

This knowledge was applied when creating the game page, linking pages and integrating visual elements. This ensured the game had a clear structure and could be expanded further if needed.

3. Game Development

Description

Game development was an important topic in this project because the application is designed as an interactive learning game rather than a static website. The goal was to teach users through active participation.

Orientation Process

We oriented ourselves in game development by thinking as a group about gameplay elements such as rounds, timers, feedback and progression. We explored how phishing scenarios could be turned into rounds where users must make decisions and receive immediate feedback.

Application in the Project

Game development concepts were applied by designing phishing scenarios as playable challenges, adding feedback messages and structuring the game so difficulty increases over time. This made the learning experience more engaging and effective.

Conclusion

By orienting ourselves in cybersecurity, software engineering and game development, we were able to combine technical knowledge with interactive learning. These ICT topics supported each other and made it possible to create an educational phishing awareness game that is both functional and engaging.